PCT/JP2005/000061

07.01.2005

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

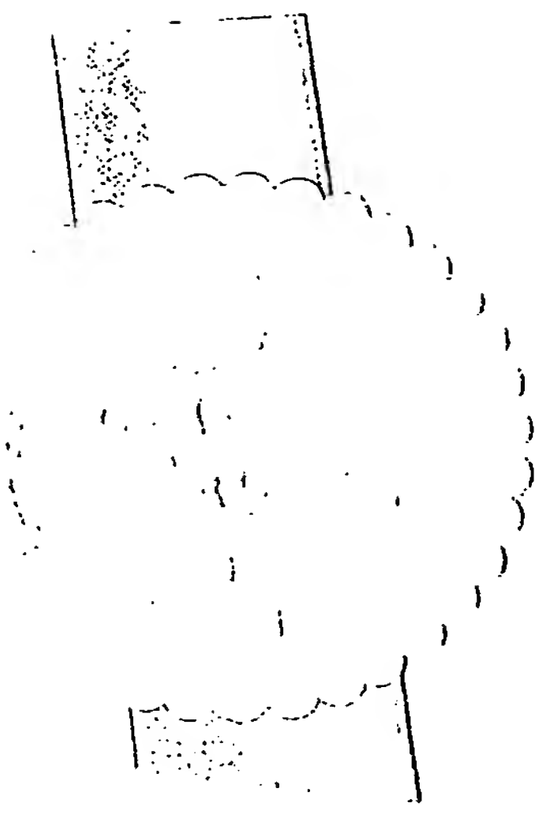
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００４年　１月　９日

出　願　番　号
Application Number:　特願２００４－００４７９８

[ST. 10/C]:　[Ｊ Ｐ ２００４－００４７９８]

出　願　人
Applicant(s):　ソニー株式会社



２００４年１２月２４日

特許庁長官
Commissioner,
Japan Patent Office　小　川　洋

出証番号　出証特２００４－３１１８００８

【書類名】　特許願
【整理番号】　0390912004
【提出日】　平成16年 1月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　5/91
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　木谷　聡
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842

【書類名】特許請求の範囲
【請求項１】
データの転送を制御する転送制御手段と、
前記転送制御手段が前記データの転送を制御した回数をカウントするカウント手段と、
前記カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断手段と、
前記第１の判断手段により前記回数が前記閾値以上になったと判断された場合、前記転送制御手段に、前記データの転送を停止するように指示を出す第１の指示手段と、
前記転送制御手段により転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、
前記転送制御手段により転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第２の判断手段と、
前記第２の判断手段により前記初期ベクトルの供給が指示されたと判断された場合、前記生成手段に前記初期ベクトルの生成を指示するとともに、前記カウンタ手段によりカウントされている前記回数をリセットするように指示を出す第２の指示手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記第１の指示手段による指示が出された場合、前記他の装置に対して前記データの転送が停止されたことを示すメッセージを出力する出力手段を
さらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、
前記第１の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第１の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、
前記第２の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第２の指示ステップと
を含むことを特徴とする情報処理方法。
【請求項４】
データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、
前記第１の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第１の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、

前記初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、
　前記第２の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第２の指示ステップと
　を含む処理をコンピュータに実行させることを特徴とするプログラム。
【請求項５】
　データの転送を制御する転送制御ステップと、
　前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
　前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、
　前記第１の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第１の指示ステップと、
　前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
　前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、
　前記第２の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第２の指示ステップと
　を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【書類名】明細書
【発明の名称】情報処理装置および方法、プログラム、並びに記録媒体
【技術分野】
【０００１】
本発明は、情報処理装置および方法、プログラム、並びに記録媒体に関し、特に、暗号化に関わる処理を実行する際に用いて好適な情報処理装置および方法、プログラム、並びに記録媒体に関する。
【背景技術】
【０００２】
さまざまな装置で、デジタルデータを授受することが一般的になりつつあるが、デジタルデータは、不正に利用されても、その質（例えば、画質や音質）が劣化しないため、不正に利用されないための対策が必要とされる。（例えば、特許文献１参照）
【０００３】
また近年普及しつつあるＤＶＤ（Digital Versatile Disc）等の記録媒体では、１枚の記録媒体（ディスク）に、例えば映画１本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると、不正なコピーを防止して著作権者の保護を図ることが益々重要になってくる。
【０００４】
そこで、例えば、ＤＶＤにビデオコンテンツを格納したＤＶＤビデオでは、著作権保護技術として、ＣＳＳ（Content Scramble System）方式が採用されている。図１は、ＣＳＳ方式を用いて暗号化されたデータが記録されている記録媒体と、その記録媒体を再生する装置の構成の一例を示す図である。
【０００５】
図１においては、記録媒体として、ディスク１１を例に挙げて図示してある。ディスク１１には、ディスク１１を識別するためのディスクキー（Secured Disc Key）２１、記録されているデータの所定の単位毎に設けられているタイトルキー（Encrypted Title Key）２２、および、データ（Scrambled Data）２３が記録されている。タイトルキー２２は、例えば、ディスク１１に映画が記録されているような場合、チャプター（Chapter）毎に設けられる。
【０００６】
ディスクキー２１とタイトルキー２２は、暗号化された状態（または、容易に読み出すことが（盗用することが）できない状態）でディスク１１に記録されている。また、データ２３は、タイトルキー２２を用いたスクランブル（Scramble）がかけられた状態でディスク１１に記録されている。
【０００７】
プレーヤ１２は、ディスク１１に記録されているキーやデータを読み出すことにより、データ２３の再生を行う。プレーヤ２３は、復号（Decrypt）部３２、復号部３３、デスクランブル（DeScramble）部３４、および、デコーダ（Decoder）３５を有する構成とされている。また、プレーヤ１２は、マスタキー（Master Key）３１を管理する管理部（不図示）も有している。
【０００８】
復号部３２は、ディスク１１から読み出されたディスクキー２１を、マスタキー３１を用いて復号し、その復号したディスクキー２１を復号部３３に供給する。復号部３３には、ディスク１１から読み出されたタイトルキー２２も供給される。復号部３３は、復号されたディスクキー２１により、暗号化されているタイトルキー２２を復号する。復号されたタイトルキー２２は、デスクランブル部３４に供給される。デスクランブル部３４には、ディスク１１から読み出されたデータ２３も供給される。
【０００９】
ディスク１１から読み出され、プレーヤ１２に供給されるデータ２３は、所定の圧縮方式（例えば、ＭＰＥＧ（Moving Picture Expert Group）方式）で圧縮され、さらにタイ

トルキー２２を用いたスクランブルがかけられた状態のものである。そこで、まず、デスクランブル部３４は、タイトルキー２２を用いて、データ２３にかけられているスクランブルを解除する。

【００１０】

スクランブルが解除されたデータ２３は、デコーダ３５に供給される。デコーダ３５は、所定のデコード方式（例えば、ＭＰＥＧ方式）により、デスクランブル部３４からのデータ２３をデコードする。デコードされたデータ３６は、図示されていないディスプレイなどに供給される。

【００１１】

図１に示したプレーヤ１２は、例えば、ＤＶＤなどのディスク１１を専用に再生するような機器であるが、そのような専用のプレーヤ１２に限らず、例えば、パーソナルコンピュータなどもディスク１１を再生する機能を有している場合がある。

【００１２】

図２は、ＤＶＤなどのディスク１１をパーソナルコンピュータなどで再生する場合の構成例を示す図である。ここでは、ディスク１１に記録されているデータを読み出す装置をドライブ装置５１とし、ドライブ装置５１により読み出されたデータを処理する装置をホスト（Host）５２と記述する。図２に示したドライブ装置５１やホスト５２には、アプリケーションなどにより実現される機能も含まれている。

【００１３】

ディスク１１には、図１に示した場合と同様に、ディスクキー２１、タイトルキー２２、および、データ２３が記録されている。ドライブ装置５１は、認証（Authentication）処理部６２、バス暗号化（Bus Encrypt）部６２、および、バス暗号化部６３を有する構成とされている。

【００１４】

ホスト５２は、認証処理部７１、バス復号（Bus Decrypt）部７２、バス復号部７３、復号（Decrypt）部７４、復号部７５、デスクランブル部７６、および、デコーダ７７を有する構成とされている。また、ホスト５２は、マスタキー３１を管理する管理部（不図示）も有している。

【００１５】

ドライブ装置５１の認証処理部５１とホスト５２の認証処理部７１は、相互認証処理を実行し、その認証処理が正常に行われたときだけ、データの授受を行う。認証処理が正常に行われると、セッションキーと称されるキーが、それぞれの認証処理部６１，７１において発行（共用）される。

【００１６】

認証処理が正常に行われた後の時点で、ディスク１１から読み出されたディスクキー２１は、ドライブ装置５１のバス暗号化部６２により暗号化される。バス暗号化部６２には、認証処理部６１において発行されたセッションキーも供給される。バス暗号化部６２は、読み出されたディスクキー２１を、セッションキーを用いて暗号化し、ホスト７１に対して出力する。

【００１７】

同様に、バス暗号化部６３は、ディスク１１から読み出されたタイトルキー２２を、認証処理部６１が発行したセッションキーを用いて暗号化し、ホスト５２に対して出力する。ディスク１１から読み出されたデータ２３は、直接的に、ドライブ装置５１からホスト５２に対して供給される。

【００１８】

ホスト５２のバス復号部７２は、ドライブ装置５１のバス暗号化部６２から供給された暗号化されているディスクキー２１を、認証処理部７１により発行されたセッションキーを用いて復号する。復号されたディスクキー２１は、復号部７４に供給される。復号部７４には、マスタキー３１も供給される。復号部７４は、バス復号部７２から供給されたディスクキー２１を、マスタキー３１を用いて復号し、その復号したディスクキー２１を復

号部７５に供給する。

【００１９】

復号部７５には、バス復号部７３からのタイトルキー２２も供給されるが、そのタイトルキー２２は、バス復号部７３が、認証処理部７１により発行されたセッションキーを用いて復号したものである。

【００２０】

復号部７５は、復号されたディスクキー２１により、暗号化されているタイトルキー２２を復号する。復号されたタイトルキー２２は、デスクランブル部７６に供給される。デスクランブル部７６には、ディスク１１から読み出されたデータ２３も供給される。

【００２１】

ディスク１１から読み出されるデータ２３は、所定の圧縮方式で圧縮され、さらにタイトルキー２２を用いたスクランブルがかけられた状態のものである。そこでまず、デスクランブル部７６は、供給されたタイトルキー２２を用いて、データ２３にかけられているスクランブルを解除する。

【００２２】

スクランブルが解除されたデータ２３は、デコーダ７７に供給される。デコーダ７７は、所定のデコード方式（例えば、ＭＰＥＧ方式）により、供給されたデータ２３をデコードする。デコードされたデータ３６は、図示されていないディスプレイなどに供給される。

【００２３】

このように、ディスク１１がセットされるドライブ装置５１と、ディスク１１に記録されているデータを処理するホスト５２により、ディスク１１に記録されているデータ２３の再生の処理が実行される場合、認証処理が行われ、その認証処理が正常に行われた後に、暗号化されたキーやデータの授受が行われる。

【００２４】

認証処理が行われた後に、実際のデータの授受が行われるのは、ドライブ装置５１とホスト５２は、所定のバス（不図示）により接続されているが、そのバスを介して授受されるデータが盗用されないようにするためである。

【００２５】

ここで、認証処理部６１と認証処理部７１との間で行われる認証処理について、図３のフローチャートを参照して説明を加える。ステップＳ１１において、ディスク１１が、ドライブ装置５１に挿入（セット）されたか否かが判断される。ステップＳ１１において、ディスク１１が、ドライブ装置５１に挿入されたと判断されるまで、待機状態が維持される（ステップＳ１１における処理が繰り返される）。

【００２６】

ステップＳ１１において、ディスク１１が、ドライブ装置５１に挿入されたと判断された場合、ステップＳ１２に処理が進められる。ステップＳ１２において、認証処理部６１と認証処理部７１により、相互認証の処理が実行される。この相互認証の処理が正常に終了されなければ、これ以降の処理は実行されない。

【００２７】

相互認証の処理が正常に終了されると、認証処理部６１と認証処理部７１のそれぞれにおいて、セッションキーが生成される。このような相互認証の処理とセッションキーの発生の処理が完了したか否かが、ステップＳ１３において判断される。ステップＳ１３において、ステップＳ１２における処理は完了したと判断されるまで、ステップＳ１２の処理が繰り返され、完了したと判断された場合、ステップＳ１４に処理が進められる。

【００２８】

ステップＳ１４において、スクランブルされたデータの授受（ドライブ装置５１からの出力）が許可された状態に設定される。この場合、スクランブルされたデータとは、データ２３（図２）のことであり、このデータ２３のドライブ装置５１からホスト５２への出力が許可された状態に設定される。

【００２９】
“許可された状態”ということについて説明を加える。データ２３の読み出しは、ホスト５２からの指示に基づいてドライブ装置５１が行う。許可される前の状態において、ドライブ装置５１は、仮にホスト５２からデータ２３の読み出し（出力）の指示を受けたとしても、エラーを返すだけで、データ２３の出力は行わない。
【００３０】
許可された後の状態においては、ホスト５２からデータ２３の読み出した指示されれば、ドライブ装置５１は、ディスク１１からデータ２３を読み出し、ホスト５２に対して出力を行う。
【００３１】
このような状態に設定されると、ディスク１１がドライブ装置５１から排出されるなどの割り込み処理が発生しない限り、スクランブルされたデータ２３の再生の処理が繰り返し行われる。
【００３２】
スクランブルされたデータ２３の出力が許可された状態にされると、ステップＳ１５において、ディスク１１がドライブ装置５１から排出された否かの判断が継続的に行われる。そして、ステップＳ１５において、ディスク１１がドライブ装置５１から排出されたと判断されると、ステップＳ１１に処理が戻され、それ以降の処理が繰り返される。
【００３３】
なお、ドライブがリセットされた場合や、電源がオフの状態にされた場合も、再生の処理が終了され、必要に応じ、ステップＳ１１に処理が戻され、それ以降の処理が繰り返される。
【００３４】
このようにして、ドライブ装置５１とホスト５２との間で認証処理が正常に終了されると、ドライブ装置５１側では、ディスク１１が排出されるまで、その挿入されているディスク１１からデータ２３を読み出し、その読み出したデータ２３をホスト５２に出力するという処理を、ホスト５２からの指示がある限り継続的に行なわれる。
【００３５】
ここで、バス暗号化部６２などの暗号化部において行われる公知の暗号化技術について説明を加える。暗号化の方式は、さまざまなものが提案されている。ここでは、ＣＢＣ（Cipher Block Chaining）方式を例に挙げて、暗号化（復号）の方式について説明する。
【００３６】
暗号化の一方式であるＣＢＣ方式は、ブロック連鎖のための一つの技法であり、排他的論理和演算により、平文の現在のブロックに暗号文の前のブロックを付加して、暗号文の各ブロックを作成する方式である。図４は、ＣＢＣ方式を用い暗号化を行う回路の一例を示す図である。
【００３７】
暗号化すべきデータは、所定の単位（例えば、ブロック暗号方式としてＡＥＳ(Advanced Encryption Standard)を用いた場合は１６バイト）毎にブロック化される。そして、第１のブロックは、排他的論理和回路１０１－１に供給され、第１のブロックに続く第２のブロックは、排他的論理和回路１０１－２に供給され、第２のブロックに続く第３のブロックは、排他的論理和回路１０１－３に供給されというように、所定の段数（ここでは、Ｎ段とする）だけ設けられた排他的論理和回路１０１－１乃至１０１－Ｎに順次、ブロック化された平文のデータが入力される。
【００３８】
排他的論理和回路１０１－１から出力された第１のブロックは、暗号化部１０２－１に供給される。暗号化部１０２－１は、鍵Ｅｋで供給された第１のブロックを暗号化する。このようにして、第１のブロックは暗号化される。
【００３９】
暗号化部１０２－１から出力された暗号化された第１のブロックは、排他的論理和回路

１０１－２にも供給され、第２のブロックとの間で排他的論理和が演算される。その結果は、暗号化部１０２－２に供給され、同じく鍵Ｅｋで暗号化される。

【００４０】

このように、ＣＢＣ方式における暗号化は、１つ前で暗号化したブロックと暗号化対象の現在の平文のブロックとの排他的論理和が演算されてから、そのブロックに対して所定の暗号化鍵での暗号化が行なわれるようになっている。結果の暗号文は次のブロックとの排他的論理和の演算に使われることになる。このように前のブロックと次々に連鎖させることにより暗号文が生成される。

【００４１】

第２のブロック以降は、前のブロックとの排他的論理和が演算されるが、第１のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第１のブロックに対しては、初期ベクトル（ＩＶ：Initializing Vector）を与えて排他的論理和を演算するように構成される。

【００４２】

次に、ＣＢＣ方式を用い復号を行う回路（例えば、バス復号部７２（図２））について、図５を参照して説明する。

【００４３】

上述したようにして暗号化されたデータは、所定の単位（例えば、ブロック暗号方式としてＡＥＳ(Advanced Encryption Standard)を用いた場合は１６バイト）毎にブロック化されている。ブロック化されているデータの内、第１のブロックは、復号部１２２－１に供給され、第１のブロックに続く第２のブロックは、復号部１２２－２に供給され、第２のブロックに続く第３のブロックは、復号部１２２－３に供給されというように、所定の段数（ここでは、Ｎ段とする）だけ設けられた復号部１２２－１乃至１２２－Ｎに順次、暗号化されたブロック単位のデータが入力される。

【００４４】

各復号部１２２－１乃至１２２－Ｎは、入力されたデータを鍵Ｄｋで復号する。各復号部１２２－１乃至１２２－Ｎから出力されたデータは、対応する排他的論理和回路１２１－１乃至１２１－Ｎに供給される。排他的論理和回路１２１－２乃至１２１－Ｎには、前の段の復号部１２２－１乃至１２２－N-1に供給されるデータも供給される。

【００４５】

このように、ＣＢＣ方式の復号は、１つ前の暗号化されているブロックと復号対象の現在の復号されたブロックとの排他的論理和が演算されることにより、最終的な復号が行われる。

【００４６】

第２のブロック以降は、前のブロックとの排他的論理和が演算されるが、第１のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第１のブロックに対しては、初期ベクトルＩＶを与えて、排他的論理和が演算される構成とされている。

【００４７】

このようにして、暗号化、復号が行われている。

【特許文献１】特許第３２５２７０６号明細書

【発明の開示】

【発明が解決しようとする課題】

【００４８】

ところで、図２に示したように、ドライブ装置５１とホスト５２によりディスク１１に記録されているデータ２３の再生の処理が実行される場合、図３のフローチャートを参照して説明したように、ドライブ装置５１とホスト５２における相互認証の処理が正常に終了されると、ドライブ装置５１からのデータ２３の出力が許可された状態にされる。

【００４９】

ここで、図６を参照して説明するに、ホスト５２側でアプリケーションＡが起動され、

そのアプリケーションＡにより、認証処理部７１で行う認証処理が実行される場合を考える。アプリケーションＡによるドライブ装置５１との認証処理が正常に実行されると、ドライブ装置５１からディスク１１からデータ２３が読み出され、出力されるといった処理が許可された状態にされる。

【００５０】

許可された状態のときに、ディスク１１がドライブ装置５１から排出されるなどの状況が発生しない限り、ドライブ装置５１からデータ２３が出力されるといった処理が許可された状態が維持される。そのような許可が維持されている状態のときに、アプリケーションＢがホスト５２側で起動されたとする。そして、アプリケーションＡにかわり、アプリケーションＢにより、データ２３の読み出しの指示などの処理が開始されたとする。

【００５１】

ドライブ装置５１とアプリケーションＢは、認証処理を行っていないにもかかわらず、ドライブ装置５１は、データ２３の出力が許可された状態に維持されているため、ドライブ装置５１からホスト５２（アプリケーションＢ）に対して、データ２３は出力されてしまう。その結果、例えば、ホスト５２が有するＨＤＤ（Hard Disc Drive）１４１にデータ２３が記憶されるといった処理が、アプリケーションＢにより実行される可能性がある。

【００５２】

このＨＤＤ１４１に対するデータ２３の記憶が不正な処理であっても、ドライブ装置５１は、アプリケーションＢの指示に基づき、データ２３を出力してしまう。よって、このような不正を防ぐことができないといった課題があった。

【００５３】

また、ＨＤＤ１４１に記憶されたデータ２３は、スクランブルがかけられた状態であるため、そのままでは再生することができないが、スクランブルを解除するアプリケーションなども存在しているため、実質的には、ＨＤＤ１４１にデータ２３が記憶された時点で、不正に利用されてしまうことを防ぐことができないといった課題があった。

【００５４】

このように、一旦、正常に認証処理が行われ、ドライブ装置５１側でデータ２３の出力が許可された状態にされると、データ２３が盗用されてしまう可能性があるといった課題があった。

【００５５】

図７を参照し、他のデータの盗用について説明する。ドライブ装置５１とホスト５２は、所定のバスにより接続され、そのバスを介してデータ２３の授受を行うように構成されている。図６を参照して説明した場合と同様に、アプリケーションＡにより、ドライブ装置５１との認証処理が行われる。そして、その認証処理が正常に行われると、ドライブ装置５１からデータ２３を出力するといった処理を実行することが許可された状態とされる。

【００５６】

バス上を授受されるデータをモニタする機能をホスト５２が有していると、そのモニタ１５１により、バス上で授受されているデータ２３をモニタする（取得する）ことが可能である。換言すれば、ドライブ装置５１から出力されたデータ２３は、アプリケーションＡとモニタ１５１に供給されるといった状態にすることが可能である。

【００５７】

そのため、ホスト５２側で、モニタ１５１により取得されたデータ２３を、ＨＤＤ１４１に記憶させるといった処理を実行することも可能となる。よって、このようにしてデータ２３が盗用されてしまう可能性もある。

【００５８】

このように、バス上を授受されるデータが、モニタ機能により盗用されてしまう可能性があるといった課題があった。

【００５９】

バス上のデータが盗用されてしまうようなことを防ぐために、バスを介して授受される
データ２３を暗号化する方法も提案されている。図８を参照して説明する。ドライブ装置
５１側からホスト５２に出力されるデータを転送データ１７１と記述する。

【００６０】

転送データ１７１は、２０４８バイト（２Ｋバイト）のデータパケット（data Packet
）とされる。上述したように、ドライブ装置５１とホスト５２は、所定のバスで接続され
ているわけだが、そのバスをコントロールするバスインタフェース１８３は、所定の単位
量のデータを取り扱うように規定されている。その単位量は、例えば、ATAPI（AT Attach
ement with Packet Interface）をバスインタフェース１８３として用いた場合、２０４
８バイトと規定されている。

【００６１】

そこで、転送データ１７１を２０４８バイトで構成されるデータパケットとした場合、
図８に示すように、１パケットは、１６バイトの初期ベクトルＩＶと２０３２バイトのデ
ータから構成される。このようなデータパケットのうち、２０３２バイトのデータ部分が
、暗号化部１８１により暗号化される。暗号化部１８１は、図８には図示していないが、
認証処理部１８１（図２）により発行されるセッションキーKsを用いて暗号化を行う。

【００６２】

暗号化部１８１は、例えば、ＣＢＣ方式を用いて暗号化を行う。ＣＢＣ方式に基づいて
暗号化を行う場合、暗号化部１８１の内部構成例は、図４に示したようになる。図４を参
照して説明したように、暗号化部１８１は、初期ベクトルＩＶも用いて暗号化を行う。す
なわち、暗号化部１８１は、転送データ１７１のデータパケットの内、２０３８バイトの
データ部分を、同じくデータパケット内に含まれる１６バイトの初期ベクトルＩＶと、認
証処理部１８１により発行されるセッションキーKsを用いて暗号化を行う。

【００６３】

暗号化部１８１により暗号化されたデータパケットも、２０４８バイトのデータである
。よって、その暗号化されたデータパケットは、バスインタフェース１８３により取り扱
うことができる。データ部分が暗号化されたデータパケットは、ホスト５２側の復号部１
８２に供給される。復号部１８２は、供給されたデータパケットに含まれる初期ベクトル
ＩＶと、認証処理部７１（図２）により発行されるセッションキーKsを用いて、暗号化さ
れているデータの復号を行う。

【００６４】

このようにして、ホスト５２側は、暗号化されたデータを受信するが、そのデータと共
に供給される初期ベクトルＩＶを用いて復号することができるため、ホスト５２側におい
て、ドライブ装置５１側から出力されたデータを再生することができる。

【００６５】

このように、バスインタフェース１８３上で授受されるデータを、暗号化されたデータ
とすることにより、仮に、バスインタフェース１８３を介して授受されるデータが盗聴さ
れても、暗号化を解くことができなければ、盗用されることがなく、結果として、データ
が不正に利用されるような不都合が発生するようなことを防ぐことが可能となる。しかし
ながら、以下のような問題点がある。

【００６６】

再度、図８を参照するに、初期ベクトルＩＶは、転送データ１７１に含まれている。転
送データ１７１に初期ベクトルＩＶを含ませる場合、ディスク１１に、他のデータと共に
書き込まれている。よって、初期ベクトルＩＶをランダムに変化させることができない（
書き込まれている初期ベクトルＩＶをそのまま用いなくてはならず、変化させることがで
きない）といった問題があった。

【００６７】

また、ディスク１１に初期ベクトルＩＶが書き込まれているのではなく、ドライブ装置
５１側でランダムに初期ベクトルＩＶを発生させ、その初期ベクトルＩＶを転送データ１
７１内に含ませるようにすることも考えられ。しかしながら、転送データ１７１に初期ベ

クトルＩＶを含ませる場合、暗号化されるデータと区別するために、例えば、ヘッダなどを付けなくてはならないなどの条件がある。

【００６８】

そのような条件があるために、ドライブ装置５１側で、ランダムに初期ベクトルＩＶを発生させるようにしても、ランダムに変化させることに対する制限があり、結果的には、ランダムに初期ベクトルＩＶを発生させるということに対してそのランダム性を保証することができない（固定パターンになってしまう）といった問題があった。

【００６９】

初期ベクトルＩＶをランダムに変化させることができない場合、換言すれば、初期ベクトルＩＶとして固定パターンが用いられるようにすると、以下のような問題が発生する可能性がある。

【００７０】

例えば、電子メールを例に挙げて考える。電子メールの書式には、宛先、送信元、件名、本文といったような一連のパターンがある。そのようなパターンがあるようなデータ（平文）を暗号化した場合、暗号化されたデータ自体もパターンがあるデータとなってしまう。第３者（攻撃者）が、そのようなパターンに注目することにより、暗号文から平文の一部を解読することが可能である。

【００７１】

また、音楽データなどで、その音楽データを繰り返し再生するような場合、結果として同じ平文を同じように暗号化することになり、暗号化されたデータ自体も同じ結果となる。そのため、上述した場合と同様に、暗号文から平分を解読することが可能である。

【００７２】

そこで、パターンがあるような平文（同一のデータを複数回暗号化するような場合）でも、暗号化されたデータ（暗号文）にパターンがないようにするために、最初のブロックに初期ベクトルＩＶを加えるようにする。初期ベクトルＩＶを加えて暗号化を実行することにより、平文のブロックに同じパターンがあっても暗号文には同じパターンが発生しないので、暗号解読を困難にさせることが出来る。また、単一の鍵で大量のデータを暗号化した場合に暗号鍵が予測しやすくなる、という解読行為を、初期ベクトルＩＶを加えて暗号化を行うようにすることで防止することができるという効果もある。

【００７３】

このような理由で最初のブロックに初期ベクトルＩＶが加えられ、その後の暗号化が行われるように構成されている場合が多い。

【００７４】

そして、初期ベクトルＩＶを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができるとされている。（参考文献：NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, APPENDIX C Generation of Counter Blocks）

【００７５】

よって、同じ初期ベクトルＩＶが繰り返し用いられると、結果として、初期ベクトルＩＶを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができないといった課題があった。

【００７６】

また、上述したように、初期ベクトルＩＶは、更新される方が好ましいといった課題があった。

【００７７】

そこで、初期ベクトルＩＶを更新できるようにした場合、図９に示すようなデータの授受の方法が考えられる。すなわち、図９に示した例では、転送データ１９１は、２０４８バイトのデータから構成され、そのデータに、１６バイトの初期ベクトルＩＶが付加され

る。そして、初期ベクトルＩＶが付加された結果、２０６４バイトにされたデータが、バスインタフェース１８３を介して授受される。

【００７８】

初期ベクトルＩＶを転送データ１９１に付加する構成とすることにより（転送データ１９１に初期ベクトルＩＶを予め含めるような構成としないことにより）、初期ベクトルＩＶを、ドライブ装置５１側でランダムに発生し、そのランダムに発生された初期ベクトルＩＶを付加させることができるようになる。

【００７９】

しかしながら、このようにして初期ベクトルＩＶをデータに付加することは、例えば２０４８バイト単位のPC Drive Interface に、２０６４バイト(ＩＶ＝１６バイトの場合)という特殊なセクタサイズを持ち込むことになり、標準的なフォーマットから外れてしまうこととなる。そのために、共通の ATAPI Device Driver を利用できない、ＵＤＦ（Universal Data Format）で扱うことのできるセクタサイズである２０４８バイトや４０９６バイトに当てはまらないためUDF FS Driverを利用できないなど、パーソナルコンピュータにおける環境との相性がよくないといった課題があった。

【００８０】

相性が良くないといったことを解決するためには、ハードウェア的に、ソフトウェア的にも特殊なものに変えなくてはならないなど、コスト的に割高になり、互換性を取りづらい、処理的に手間がかかるといった課題もあった。

【００８１】

本発明はこのような状況に鑑みてなされたものであり、認証処理が正常に終了し、ドライブ装置側からデータが出力されることが許可された状態にされた後においても、その許可状態を解除できるようにし、データの盗用を防ぐことを目的とする。また、汎用なバスを用いた場合においても、初期ベクトルＩＶを更新できるようにし、そのバス上で授受されるデータが盗用されないようなセキュリティを高めることを目的とする。

【課題を解決するための手段】

【００８２】

本発明の情報処理装置は、データの転送を制御する転送制御手段と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断手段と、第１の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第１の指示手段と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第２の判断手段と、第２の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第２の指示手段とを備えることを特徴とする。

【００８３】

前記第１の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段をさらに備えるようにすることができる。

【００８４】

本発明の情報処理方法は、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、第１の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第１の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理

で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、第２の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第２の指示ステップとを含むことを特徴とする。

【００８５】

本発明のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、第１の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第１の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、第２の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第２の指示ステップとを含む処理をコンピュータに実行させることを特徴とする。

【００８６】

本発明の記録媒体のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断ステップと、第１の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第１の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第２の判断ステップと、第２の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第２の指示ステップとを含むことを特徴とする。

【００８７】

本発明の情報処理装置および方法、並びにプログラムにおいては、初期ベクトルの供給の指示が定期的に行われなければ、データの授受が停止される。

【発明の効果】

【００８８】

本発明によれば、装置間での転送路上におけるセキュリティを高めることが可能となる。

【００８９】

また、本発明によれば、記録媒体を扱う装置とその装置からのデータを扱う他の装置との間で認証処理が行われた後、記録媒体を扱う装置側で、記録媒体から読み出したデータを他の装置に出力することが許可された状態にされても、その状態を解除（更新）することが可能となる。もって、一旦、他の装置へのデータの出力が許可された状態であっても、その後の不正なアクセスによるデータの流出を防ぐことが可能となる。

【００９０】

また、本発明によれば、暗号化の際に用いられる初期ベクトルをランダムに更新することができ、同一のデータを暗号化しても、同一の暗号文が生成されるようなことを防ぐことが可能となる。もってデータのすり替え、データの改竄行為などの不正な処理を防止することができる。

【００９１】
また、本発明によれば、初期ベクトルを更新するようにしても、汎用のバスインタフェースおよびOS(Operating System)で標準的に用意されたUDF FS Driverを利用できる。もって、初期ベクトルを更新できるようにするために、装置間の環境を変更しなくてはならないといったような不都合が発生するようなことを防ぐことができる。
【発明を実施するための最良の形態】
【００９２】
以下に本発明の最良の形態を説明するが、開示される発明と実施の形態との対応関係を例示すると、次のようになる。明細書中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。
【００９３】
さらに、この記載は、明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現し、追加される発明の存在を否定するものではない。
【００９４】
本発明を適用した情報処理装置は、データの転送を制御する転送制御手段（例えば、図１３のステップＳ４６の処理を実行する図１０のセクタ転送制御部３１３）と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段（例えば、図１３のステップＳ４７の処理を実行する図１０のセクタ転送カウンタ３１４）と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第１の判断手段（例えば、図１３のステップＳ４５の処理を実行する図１０のセクタ転送カウンタ３１４）と、第１の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第１の指示手段（例えば、図１０のセクタ転送カウンタ３１４）と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段（例えば、図１３のステップＳ４１の処理を実行する図１０の乱数発生部３１５）と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第２の判断手段（例えば、図１３のステップＳ４０の処理を実行する図１０のコマンド処理部３１７）と、第２の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第２の指示手段（例えば、図１３のステップＳ４２の処理を実行する図１０の乱数発生３１５）とを少なくとも備える。
【００９５】
前記第１の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段（例えば、図１３のステップＳ４８の処理を実行する図１０のメッセージ伝達部３１６）をさらに備える。
【００９６】
以下に、本発明の実施の形態について図面を参照して説明する。
【００９７】
図１０は、本発明を適用したシステムの一実施の形態の構成を示す図である。
【００９８】
図１０に示したシステムは、所定の記録媒体に記録されたデータを再生する（読み出す）システムの構成例を示している。図１０に示したシステムは、データを供給するドライブ装置３０１と、データの供給を受けるホスト３０２から構成されている。
【００９９】
ディスク３０３は、例えば、CD-ROM（Compact Disc-ROM）、CD-R（Compact Disc-Reco

rdable）、CD-RW（Compact Disc-ReWritable）、DVD-ROM（Digital Versatile Disc-ROM）、DVD-R（Digital Versatile Disc-Recordable）、DVD-RW（Digital Versatile Disc-Rerecordable）、DVD+R（DVD+Recordable）、DVD+RW（DVD+ReWritable）、DVD-RAM（Digital Versatile Disk-Random Access Memory）、Blu-Ray Discなどである。また、本発明の適用範囲はこれらの記録媒体に限定されるものではなく、他の形態（記録方式、形状など）の記録媒体を扱うシステムにも適用可能である。

【０１００】

ドライブ装置３０１とホスト３０２は、所定のインタフェースによりデータの授受が行えるように接続されている。所定のインタフェースとしては、例えば、ＡＴＡＰＩ（ATAttachment with Packet Interface）を用いることができる。ＡＴＡＰＩは、ＩＤＥ（Integrated Drive Electronics）や、ＡＴＡ（AT Attachment）インタフェースにＣＤ－ＲＯＭドライブなどハードディスク以外の周辺機器を接続するためのデータ転送方式に従ったインタフェースであり、例えばＳＣＳＩから流用したコマンドをパケット化してＩＤＥインタフェースに渡すことで周辺機器の制御を可能とする。同様のコマンドパケットはＵＳＢ（Universal Serial Bus）や IEEE1394 などの物理インタフェースへも適用可能である。

【０１０１】

ドライブ装置３０１は、認証処理部３１１、暗号化部３１２、セクタ転送制御部３１３、セクタ転送カウンタ３１４、乱数発生部３１５、メッセージ伝達部３１６、コマンド処理部３１７、および、アクセス処理部３１８を含む構成とされている。

【０１０２】

ホスト３０２は、認証処理部３２１、復号部３２２を含む構成とされている。

【０１０３】

ドライブ装置３０１の認証処理部３１１とホスト３０２の認証処理部３２１により、相互認証に関わる処理が実行される。

【０１０４】

暗号化部３１２には、アクセス処理部３１８による処理により、ディスク３０３から読み出されたセクタデータ３５１と、認証処理部３１１からセッションキーKsが供給される。また、暗号化部３１２には、乱数発生部３１５により発生された乱数が、初期ベクトルＩＶとして供給される。

【０１０５】

なお、乱数発生部３１５により発生された乱数を、そのまま初期ベクトルＩＶとして用いても良いが、乱数と他のデータ（例えば、ディスク３０３から読み出されるＰＳＮ（Physical Sector Number）など）が用いられて生成されるものを初期ベクトルＩＶとして用いられるようにしても良く、そのような処理を実行する部分を、ドライブ装置３０１内に設けるようにしても良い。

【０１０６】

暗号化部３１３は、供給されたセクタデータ３５１をセッションキーKsと初期ベクトルＩＶを用いて暗号化し、セクタ転送制御部３１３に供給する。セクタ転送制御部３１３は、暗号化されたセクタデータ３５１を、ホスト３０３の復号部３２２に対して供給する。よって、ドライブ装置３０１からホスト３０３に供給されるデータは、暗号化されたセクタデータ３５１である。

【０１０７】

暗号化部３１２からは、セクタ転送カウンタ３１４にもデータが出力される。セクタ転送カウンタ３１４は、ホスト３０２に対して出力されたセクタデータ（暗号化部３１２から出力されたセクタデータ３５１）の数をカウントするように構成されている。換言すれば、セクタ転送カウンタ３１４は、セクタ転送制御部３１３がセクタデータの転送を制御した回数をカウントする。

【０１０８】

また、セクタ転送カウンタ３１４は、予め設定されたカウント数の最大値（Nmaxとす

る）を管理しており、カウントしているセクタ数（カウンタ値N）が、その最大値を超えないか否かを常に監視している。

【０１０９】

セクタ転送カウンタ３１４は、N≧Nmaxになった場合、セクタ転送制御部３１３に対して、ホスト３０２へのセクタデータ３５１の出力を停止するように指示を出す。このような指示を出すとともに、セクタ転送カウンタ３１４は、コマンド処理部３１７に対して、アクセス処理部３１８によるディスク３０３へのアクセスを停止するように指示を出す。

【０１１０】

セクタ転送制御部３１３は、セクタ転送カウンタ３１４からセクタデータ３５１の出力の停止の指示を受けた場合、メッセージ伝達部３１６に対して、メッセージ３６２（この場合、エラーメッセージ）をホスト３０２に対して出力するように指示を出す。

【０１１１】

一方、ホスト３０３の復号部３２２は、ドライブ装置３０１からインタフェースを介して暗号化されたセクタデータ３５１の供給をうける。復号部３２２は、ドライブ装置３０１から、セクタデータ３５１とは別の経路（詳細は図１１を参照して後述する）で、乱数発生部３１５により発生された初期ベクトルＩＶも供給される。

【０１１２】

復号部３２２は、認証処理部３３１から供給されるセッションキーKsと、ドライブ装置３０１から供給された初期ベクトルＩＶを用いて復号処理を実行し、セクタデータ３６１を生成する。

【０１１３】

ホスト３０２からは、コマンドパケット３６３が必要に応じて、ドライブ装置３０１に対して供給される。このコマンドパケット３６３は、例えば、ディスク３０３からデータの読み出しを指示するリードコマンド（Read command）、ディスク３０３へのデータの書き込みを指示するライトコマンド（Write command）、初期ベクトルＩＶの発行を指示するレポートキーコマンド（Report Key command）などがある。

【０１１４】

図１１を参照して、セクタデータ３５１が授受される経路と、その他のデータが授受される経路について説明する。PC driver３９１は、例えば、初期ベクトルＩＶの生成、暗号化セクタデータの作成、転送セクタデータの作成などを制御するドライバーである。PC driver３９１からのデータは、Optical Disc driver３９２に渡される。

【０１１５】

Optical Disc driver３９２は、光ディスク（Optical Disc）の読み出しや書き込みを制御するドライバーである。光ディスクがDVDなどの記録媒体である場合、その光ディスクに書き込まれているデータ（ファイル）は、UDF（Universal Data Format）に準拠したものとされている。よって、Optical Disc driver３９２により読み出された（制御された）データ（ファイル）は、UDF FS driver３９３の制御により、Optical Disc file reader３９４を介して、Video/Audio Playback function３９５に渡される。

【０１１６】

Video/Audio Playback function３９５は、例えば、転送セクタデータの取得、初期ベクトルＩＶの取得、暗号化セクタデータの復号を制御する。

【０１１７】

このように、セクタデータなどの映像や音声に関わるデータは、UDF FS driver３９３を介して授受されるが、その他の、例えば、初期ベクトルＩＶやその初期ベクトルＩＶを発行させるためのコマンドなどのデータは、UDF FS driver３９３を介さずに授受される。このUDF FS driver３９３を介さずに行われるデータの授受の経路は、Microsoft Windows（登録商標）においてはSCSI PASS Throughなどと称されている。

【０１１８】

図１０において、ドライブ装置３０１とホスト３０２との間に図示されている線のうち

、太線で示した経路が、UDF FS driver３９３を介してデータの授受が行われる経路（以下、適宜、UDF経路と称する）を示し、細線で示した経路が、その他のデータの授受が行われる経路（SCSI PASS Through、以下、適宜、パス経路と称する）を示すとする。

【０１１９】

図１０に示したように、セクタ転送制御部３１３から復号部３２２へのUDF経路である。認証処理部３１１と認証処理部３２１との間で行われる認証処理に必要とされるデータの授受は、パス経路を介して行われる。また、メッセージ伝達部３１６から出力されるメッセージ３６２は、パス経路を介して授受される。また、初期ベクトルＩＶも、パス経路を介して授受される。

【０１２０】

UDF FS driver３９３は、２０４８バイトのデータ、または、２０４８バイトの整数倍のデータ容量のデータを取り扱う。よって、UDF経路を介して授受されるデータは、２０４８バイトまたはその倍数のデータしか通すことができない。

【０１２１】

これに対し、パス経路は、基本的にデータの容量にかかわらず授受することが可能である。よって、１６バイトで構成される初期ベクトルＩＶなどを授受をするのに適した経路である。

【０１２２】

図１０に示した構成のドライブ装置３０１の動作について、図１２と図１３のフローチャートを参照して説明する。ステップＳ３１において、ドライブ装置３０１にディスク３０３が、挿入されたか否かが判断される。ステップＳ３１において、ドライブ装置３０１にディスク３０３が挿入されたと判断された場合、ステップＳ３２に処理が進められ、ホスト３０２において所定のアプリケーションが起動されたか否かが判断される。

【０１２３】

所定のアプリケーションとは、ドライブ装置３０１に挿入されたディスク３０３からデータを読み出す、または、書き込むために必要とされるアプリケーションである。

【０１２４】

ステップＳ３２において、ホスト３０２において所定のアプリケーションが起動されたと判断された場合、ステップＳ３３に処理が進められる。ステップＳ３３において、ドライブ装置３０１とホスト３０２との間で相互認証処理が実行され、セッションキーＫｓが、ドライブ装置３０１とホスト３０２で、それぞれ生成（共用）される。ステップＳ３４において、セッションキーＫｓの生成が完了したか否かが判断される。セッションキーＫｓの生成が完了されるまで、ステップＳ３３とステップＳ３４の処理が繰り返される。

【０１２５】

そして、ステップＳ３４において、セッションキーＫｓの生成が完了したと判断されると、ステップＳ３５に処理が進められ、ドライブ装置３０１のセクタ転送カウンタ３１４のカウンタ値Ｎが、予め設定されているカウンタ値Ｎの最大値である値Ｎmaxに設定される（Ｎ＝Ｎmaxに設定される）。

【０１２６】

このように、Ｎ＝Ｎmaxに設定されると、セクタ転送カウンタ３１４の指示により、セクタ転送制御部３１３からホスト３０２へのデータの出力が許可されない状態に設定される。

【０１２７】

ステップＳ３６において、ホスト３０２から初期ベクトルＩＶの転送要求があったか否かが判断される。この判断は、コマンド処理部３１７が、ホスト３０２側から、コマンドパケット３６３を受信したか否かを判断し、かつ、受信したコマンドパケット３６３が、初期ベクトルＩＶの転送要求を示すものであるか否かを判断することにより行われる。

【０１２８】

ステップＳ３６において、初期ベクトルＩＶの転送要求があったと判断されるまで、ステップＳ３６の処理が繰り返される。そして、ステップＳ３６において、初期ベクトルＩ

Ｖの転送要求があったと判断された場合、ステップ３７に処理が進められ、初期ベクトルＩＶの生成が行われる。

【０１２９】

コマンド処理部３１７は、ホスト３０２からのコマンドパケット３６３を受信し、そのコマンドパケット３６３を解析することにより、初期ベクトルＩＶの転送要求であると判断すると、そのことを、乱数発生部３１５に知らせる。そのような知らせを受けた乱数発生部３１５は、ステップＳ３７の処理として、初期ベクトルＩＶを生成する。

【０１３０】

乱数発生部３１５は乱数を発生するが、その乱数が、そのまま初期ベクトルＩＶとされる。または、発生された乱数と所定の情報（例えば、初期ベクトルＩＶの転送要求を指示するコマンドパケット３６３に含まれる情報）などを用い、排他的論理和を算出するなどの処理が実行されることにより、初期ベクトルＩＶが発生されるようにしても良い。

【０１３１】

乱数発生部３１５は、初期ベクトルＩＶを生成すると共に、セクタ転送カウンタ３１４に対して、カウンタ数Ｎを０に設定し直すように指示を出す。このような指示を受け取ったセクタ転送カウンタ３１４は、ステップＳ３８の処理として、カウンタ値Ｎを０に設定し直す。このようにセクタ転送カウンタ３１４のカウンタ値Ｎが、０に設定されると、セクタ転送制御部３１３からのデータの出力が許可された状態に変更される。

【０１３２】

乱数発生部３１５により生成された初期ベクトルＩＶは、ステップＳ３９において、ホスト３０２に供給される。この初期ベクトルＩＶの供給（転送）は、パス経路を介して行われるため、例えば、初期ベクトルＩＶが１６バイトで構成される場合であっても、その１６バイトの初期ベクトルＩＶをドライブ装置３０１とホスト３０２側で授受することが可能である。

【０１３３】

ステップＳ３３乃至Ｓ３９の処理のうち、初期ベクトルＩＶの授受に関わる処理について、図１４を参照して説明を加える。

【０１３４】

ホスト３０２は、ステップＳ１０１において、ドライブ装置３０１は、ステップＳ１１１において、それぞれ相互認証（Authentication）を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置３０１の認証処理部３１１とホスト３０２の認証処理部３２１との、それぞれにおいてセッションキーＫｓが生成される（共有される）ことになる。

【０１３５】

ホスト３０２は、ステップＳ１０２において、コマンドパケット３６３を生成し、ドライブ装置３０１に対して出力する。ステップＳ１０２において生成され、出力されるコマンドパケット３６３は、REPORT KEY commandであり、このREPORT KEY commandは、ここでは、初期ベクトルＩＶの転送を要求するものであるとする。

【０１３６】

そのようなREPORT KEY commandを、ステップＳ１１２の処理として受信したドライブ装置３０１は、ステップＳ１１３において、初期ベクトルＩＶを生成する。生成された初期ベクトルＩＶは、ステップＳ１１４において、ドライブ装置３０１からホスト３０２に対して出力される。この出力される初期ベクトルＩＶは、そのままホスト３０２側に出力される。

【０１３７】

このようにしてドライブ装置３０１から出力された初期ベクトルＩＶを、ホスト３０３は、ステップＳ１０３において受信する。

【０１３８】

このように、ドライブ装置３０１からホスト３０２に転送される初期ベクトルＩＶを、暗号化などの処理を施さずに、そのまま転送されるようにしても良いが、暗号化が施され

た状態で転送されるようにしてももちろん良い。

【０１３９】

初期ベクトルＩＶは、乱数発生部３１５により乱数を用いて発生されるため、ランダムに変化される値である。また、初期ベクトルＩＶは、セッションキーKsと異なり、秘匿する必要性は低いと考えられる。このようなことを考慮し、図１４を参照して説明したように、転送される初期ベクトルＩＶは、そのまま転送されるようにしても良い。

【０１４０】

しかしながら、初期ベクトルＩＶは、予測不可能であることが好ましいという条件がある。その条件を満たすために、転送される初期ベクトルＩＶを暗号化し、より安全性を高めるようにしてももちろん良い。

【０１４１】

より安全性を高めて初期ベクトルＩＶが転送されるようにした場合、図１５に示すように処理が行われる。ホスト３０２側で行われるステップＳ１３１乃至Ｓ１３３における処理は、基本的に、図１４におけるステップＳ１０１乃至Ｓ１０３と同様に行われるが、ステップＳ１０３において受信される初期ベクトルＩＶは、暗号化されているため、受信された後に、復号という処理が実行される点が異なる。

【０１４２】

ドライブ装置３０１側で行われるステップＳ１４１乃至Ｓ１４４における処理も、基本的に、図１４におけるステップＳ１１１乃至Ｓ１１４と同様であるが、ステップＳ１４３において、初期ベクトルＩＶが生成されたあと、その初期ベクトルＩＶが、セッションキーKsが用いられて暗号化され、その暗号化された初期ベクトルＩＶ（Ｅ［Ks，IV］）が、ステップＳ１４４における処理としてホスト３０２側に転送される点が異なる。

【０１４３】

このようにして、ホスト３０２側から初期ベクトルＩＶの転送要求があると、ドライブ装置３０１は、初期ベクトルＩＶを生成し、ホスト３０２側に転送する。もちろん、ドライブ装置３０１は、生成した初期ベクトルＩＶを、ホスト３０２側に転送するだけでなく、自己の暗号化部３１２（図１０）にも供給する。

【０１４４】

図１２のフローチャートの処理の説明に戻り、ステップＳ３９における初期ベクトルＩＶの転送の処理が終了されると、ステップＳ４０（図１３）に処理が進められる。ステップＳ４０において、初期ベクトルＩＶの再発行要求があったか否かが判断される。ステップＳ４０において、初期ベクトルＩＶの再発行要求があったと判断された場合、ステップＳ４１乃至Ｓ４３の処理が実行される。

【０１４５】

ステップＳ４１乃至Ｓ４３は、基本的に、ステップＳ３７乃至ステップＳ３８の処理と同様であるが、図１６を参照して説明を加える。ホスト３０１は、ステップＳ１６１において、初期ベクトルＩＶの再発行要求をドライブ装置３０１に対して出す。この再発行要求は、コマンドパケット３６３が出力されることにより行われるが、このコマンドパケット３６３は、例えば、図１４のステップＳ１０２において発行されるREPORT KEY commandと同じである。

【０１４６】

ドライブ装置３０１は、ステップＳ１７１において、REPORT KEY commandを受信すると、ステップＳ１７２において、初期ベクトルＩＶを再生成する。初期ベクトルＩＶの再生成は、図１４のステップＳ１１３、または、図１５のステップＳ１４３の処理と同様に行われる。そして、再生成された初期ベクトルＩＶは、ステップＳ１７３において、ホスト３０２側に転送される。この転送時に、初期ベクトルＩＶは、暗号化が施されて転送されるようにしても良いし、そのまま転送されるようにしても良い。

【０１４７】

図１３のフローチャートの説明に戻り、ステップＳ４０において、初期ベクトルＩＶの再発行要求はないと判断された場合、または、ステップＳ４３における処理として初期ベ

クトルＩＶの転送に関わる処理が終了した場合、ステップＳ４４に処理が進められる。

【０１４８】

ステップＳ４４において、セクタデータ３５１の転送要求があったか否かが判断される。この判断は、コマンド処理部３１７が、ホスト３０２側から、コマンドパケット３６３を受信したか否かを判断し、かつ、受信したコマンドパケット３６３が、セクタデータ３５１の転送を要求するものであるか否かを判断することにより行われる。

【０１４９】

ステップＳ４４において、セクタデータ３５１の転送要求はないと判断された場合、ステップ４０に処理が戻され、それ以降の処理が繰り返される。一方、ステップＳ４４において、セクタデータ３５１の転送要求があったと判断された場合、ステップ４５に処理が進められる。

【０１５０】

ステップＳ４５において、セクタ転送カウンタ３１４のカウンタ値Ｎが、Ｎ＞Ｎmaxという関係を満たすか否かが判断される。ステップＳ４５において、Ｎ＞Ｎmaxという関係は満たされていないと判断された場合、ステップＳ４６に処理が進められる。Ｎ＞Ｎmaxという関係が満たされていない状態、すなわち、Ｎ＜Ｎmaxという関係を満たす状態のときには、セクタ転送制御部３１３からのデータの出力（ホスト３０２側へのデータの転送）が許可されている状態である。

【０１５１】

そこで、ステップＳ４６においては、セクタ転送制御部３１３からホスト３０２側へのデータの転送が行われる。まず、コマンド処理部３１７の指示により、アクセス処理部３１８が、ディスク３０３からセクタデータ３５１の読み出しの制御を行う。アクセス処理部３１８の制御により、ディスク３０３から読み出されたセクタデータ３５１は、暗号化部３１２に供給される。

【０１５２】

暗号化部３１２は、認証処理部３１１から供給されるセッションキーKsと、乱数発生部３１５から供給される初期ベクトルＩＶを用いて、セクタデータ３５１を暗号化する。暗号化されたセクタデータ３５１は、セクタ転送制御部３１３の制御により、ホスト３０２に転送される。この際、セクタデータ３５１が転送される経路は、UDF経路であり、そのデータ量は、２０４８バイト（または、２０４８の整数倍のバイト数）とされている。

【０１５３】

暗号化部３１２からデータが出力されると、その情報は、セクタ転送カウンタ３１４に供給される。セクタ転送カウンタ３１４は、ステップＳ４７において、自己が管理しているカウンタ値Ｎを、Ｎ＋１の値に更新し、その更新された値を新たなカウンタ値Ｎと設定する。セクタ転送カウンタ３１４におけるカウンタ値Ｎの更新が終了されると、ステップＳ４０に処理が戻され、それ以降の処理が繰り返される。

【０１５４】

このセクタデータ３５１の転送に関わる処理について、図１７のタイミングチャートを参照して、説明を加える。ホスト３０２は、ステップＳ２０１において、リードコマンド（READ command）を発行する。リードコマンドは、ディスク３０３からセクタデータ３５１を指示する際に発行されるコマンドである。また、後述するように、ディスク３０３にデータを書き込む際にはライトコマンド（WRITE command）が発行される。

【０１５５】

発行されるリードコマンドは、例えば、図１８に示したデータ構成を有するコマンドパケット３６３の一種である。コマンドの詳細はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。

【０１５６】

図１８に示したコマンドパケット３６３は、リードコマンドまたはライトコマンドの形式を示すものである。図１８に示したコマンドパケット３６３内のデータのうち、以下の説明に必要な部分のデータについて説明を加える。

【０１５７】
“Operation Code”には、リードコマンドであるか、ライトコマンドであるかを示すデータが書き込まれる。よって、この部分に書き込まれているデータを参照することで、ホスト３０２からコマンドを受け取ったドライブ装置３０１は、リードコマンドであるか、ライトコマンドであるかを判別することが可能となっている。また、“Operation Code”は、１バイトのデータである
【０１５８】
“Logical Block Address”には、コマンドパケット３６３がリードコマンドである場合には、読み出すべきアドレスの開始ＬＢＡが書き込まれ、コマンドパケット３６３がライトコマンドである場合には、書き込むべきアドレスの開始ＬＢＡが書き込まれている。また、“Logical Block Address”は、４バイトのデータである。
【０１５９】
“Transfer Length”には、コマンドパケット３６３がリードコマンドである場合には、読み出しセクタ数を指示するデータが書き込まれ、コマンドパケット３６３がライトコマンドである場合には、書き込みセクタ数を指示するデータが書き込まれる。また、“Transfer Length”は、４バイトのデータである。
【０１６０】
ステップＳ２０１において、ホスト３０２から発行されるコマンドパケット３６３は、“Operation Code”がリードコマンドを示す値が記載されているコマンドである。ここでは、その発行されるリードコマンドに含まれる“Transfer Length”は“Ｎ１”であるコマンドが発行されたとする。
【０１６１】
ステップＳ２０１における処理で発行されたリードコマンドは、ステップＳ２３１において、ドライブ装置３０１のコマンド処理部３１７に供給される。コマンド処理部３１７は、供給されたコマンドの“Operation Code”を参照し、リードコマンドであることを認識する。そして、“Logical Block Address”を参照し、データの読み出しを開始するアドレスを認識し、“Transfer Length”を参照して、この場合、“Transfer Length”＝Ｎ３ということを認識する。
【０１６２】
コマンド処理部３１７は、認識結果を、アクセス処理部３１８に供給する。アクセス処理部３１８は、コマンド処理部３１７からの認識結果に基づき、ディスク３０３からのデータの読み出しを制御する。アクセス処理部３１８における処理としては、アドレスの変換処理などがある。
【０１６３】
アクセス処理部３１８は、LBA/PSN変換を行う。ＬＢＡは、Logical Block Addressの略であり、ＰＳＮは、Physical Sector Numberの略である。ＬＢＡは、論理的なアドレスを示し、例えば、リードコマンドに含まれ、ディスク３０３上の読み出すべきデータの物理媒体に依存せずにドライブ装置３０１とホスト３０２との間で共通的に扱うことを可能とする論理的なアドレスを示す。
【０１６４】
ＬＢＡに対し、ＰＳＮは、物理的なアドレスを示す。コマンドパケット３６３には、ＬＢＡが含まれるが、このＬＢＡは、ディスク３０３上の論理的なアドレスを示し、実際の物理的なアドレスは示していないため、物理媒体から読み出した物理的なアドレスを示すＰＳＮから共通に扱える論理的なアドレスへ変換するといった処理が、必要に応じ行われる。その変換処理を、アクセス処理部３１８は行う。
【０１６５】
なお、ディスク３０３上のユーザに開放された記録領域であるユーザデータエリア（不図示）の物理セクタに対して、例えば、ある物理セクタ番号の物理セクタを基準として、シーケンシャルな論理セクタ番号の論理セクタが、順次割り当てられる。変換方法の事例はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。

【０１６６】
ＬＢＡがＰＳＮに変換されると、ステップＳ２３２の処理として、その変換されたＰＳＮが指し示すディスク３０３上の位置が検索される。この検索の結果、ピックアップ（不図示）がディスク３０３上の、読み出すべき位置に移動されるなどの処理が実行され、ディスク３０３からセクタデータ３５１が読み出される。読み出されたセクタデータ３５１は、暗号化部３１２に供給される。

【０１６７】
暗号化部３１２には、認証処理部３１１からセッションキーKsが供給され、乱数発生部３１５から初期ベクトルＩＶも供給される。暗号化部３１２は、供給されたセッションキーKsと初期ベクトルＩＶを用いてセクタデータ３５１を暗号化する。暗号化されたセクタデータ３５１（この場合、Encrypted Sector Data ＃１）は、ステップＳ２３２の処理として、セクタ転送制御部３１３の制御のもと、ホスト３０２の復号部３２２に対して出力される。

【０１６８】
復号部３２２は、供給されたEncrypted Sector Data ＃１を、認証処理部３２１から供給されるセッションキーKsと、ドライブ装置３０１の乱数発生部３１５から供給された初期ベクトルＩＶを用いて復号し、セクタデータ３６１を生成する。このようにして生成されたセクタデータ３６１は、図示されていないアプリケーションソフトウェアやディスプレイやスピーカに提供される。

【０１６９】
このような処理がドライブ装置３０１とホスト３０２間で繰り返される。ドライブ装置３０１から、順次、Physical Sector Data が読み出される。すなわち、ディスク３０３側からは、ドライブ装置３０１の検索制御に応じて順次、連続的にセクタデータが読み出されドライブ装置３０１に供給される。

【０１７０】
ドライブ装置３０１は、ステップＳ２３３乃至Ｓ２４０の各ステップの処理において、順次、読み出したセクタデータを暗号化し、ホスト３０２の要求（リードコマンドの発行）に応じてホスト３０２に供給する。

【０１７１】
ドライブ装置３０１は、ホスト３０２に対してセクタデータを転送する際、セクタ転送カウンタ３１４により管理されているカウンタ値Ｎの更新処理なども行う。例えば、ステップＳ２３２の処理として、セクタデータ３５１が暗号化されてホスト３０２側に転送されると、セクタ転送カウンタ３１４のカウンタ値Ｎは、１だけ増加された値に更新される（ステップ４７の処理）。よって、このようなカウンタ値Ｎの更新の処理が繰り返される（セクタデータが、順次、ホスト３０２側に転送されると）、カウンタ値Ｎの値が、閾値Nmaxよりも大きくなる（Ｎ＞Nmaxを満たす）ときがある。

【０１７２】
図１７を参照するに、（Ｎ１＋Ｎ２）＜Nmax＜（Ｎ１＋Ｎ２＋Ｎ３）と設定されていたとする。このような場合、ステップＳ２４０において、（Ｎ１＋Ｎ２＋１）番目のセクタデータが出力された後の時点（セクタ転送カウンタ３１４が管理するカウンタ値Ｎが、（Ｎ１＋Ｎ２＋１）となった後の時点）で、継続的に、セクタデータがディスク３０３から読み出され、暗号化され、転送されという処理が繰り返されると、カウンタ値Ｎの値は、順次１つづ増加されるので、Ｎ＞Nmaxという条件を満たすようになる。

【０１７３】
Ｎ＞Nmaxという条件が満たされると、すなわち、ステップＳ４５（図１３）において、ＹＥＳと判断されると、ステップＳ４８（図１７においては、ステップＳ２４１）に処理が進められる。

【０１７４】
ステップ４８（ステップＳ２４１）において、エラーメッセージ（Error Message）がドライブ装置３０１からホスト３０２側に出力される。ドライブ装置３０１のセクタ転送

カウンタ３１４は、自己がカウントしているカウンタ値Ｎが、閾値Ｎmaxよりも大きくなったと判断したとき、セクタ転送制御部３１３に対して、暗号化部３１２から供給されるデータをホスト３０１側に出力しないように指示を出す。

【０１７５】

セクタ転送制御部３１３は、セクタ転送カウンタ３１４から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部３１６に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部３１６は、セクタ転送制御部３１３から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト３０２に対して送信する。このエラーメッセージは、ホスト３０２に、指示されたデータの供給はできないということを認識させるためのメッセージである。

【０１７６】

このようなメッセージが出力されると、ドライブ装置３０１側からはデータが出力されない状態とされる。換言すれば、ドライブ装置３０１側で、認証処理が正常に行われた結果、データの出力が許可された状態であっても、その状態が解除され、許可されない状態に変更される。

【０１７７】

このように、本実施の形態によれば、一度設定されたデータ出力の許可という状況を変更することが可能である。よって、エラーメッセージが出力された後、ホスト３０２から、ディスク３０３からのデータの読み出しが指示されても、その指示に対応して、データが読み出されることはない。

【０１７８】

エラーメッセージが出力されると、ドライブ装置３０１からホスト３０２へのデータの出力が停止される。このようなデータの出力が停止されてしまうような状況が発生しないようにするためには、ホスト３０２側で、初期ベクトルＩＶの発行要求が、所定のタイミングでドライブ装置３０１に対して出されればよい。

【０１７９】

すなわち、初期ベクトルＩＶの発行が要求されれば（例えば、ステップＳ４０（図１３））、セクタ転送カウンタ３１４のカウンタ値Ｎが０にリセットされる（ステップＳ４２）。その結果、Ｎ＞Ｎmaxという条件が満たされることを回避できるため、エラーメッセージが出力されるような状況が発生する（ステップＳ４８）ようなことを回避することができる。

【０１８０】

ホスト３０２は、定期的に初期ベクトルＩＶの発行の要求を出す。定期的とは、例えば、初期ベクトルＩＶの発行を要求した後、転送を指示したデータ量の累計が所定のデータ量（例えば、１６Mbyte（８K Sector））を超える毎に要求されるということである。または、初期ベクトルＩＶの発行を要求した後、所定の時間が経過する毎に要求されるということである。

【０１８１】

いずれにしても、ホスト３０２は、所定のタイミングで、初期ベクトルＩＶの発行の要求を出す。よって、正常に（正当に）処理が実行されている間、ドライブ装置３０１側では、ステップＳ４１乃至Ｓ４３の処理が定期的に行われることになり、定期的にセクタ転送カウンタ３１４のカウンタ値Ｎが０に設定されることになる。

【０１８２】

このようにすることで、少なくとも以下のような問題を解決することができる。

ドライブ装置３０１とホスト３０２との間で一旦、相互認証が成功したら、ドライブ装置３０１は、相手（ホスト３０２において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題。

バスを第３者が観測し、保護されたデータを横取りして解読し平文化してしまうといった問題（不正に利用されてしまうという問題）。

【０１８３】
このような問題を解決するために、上述したように、まず、保護されたデータ（ディスク３０３に記録されているセクタデータ３５１）をドライブ装置３０１からホスト３０２にバス転送する際、その保護されたデータをセッションキーKsで暗号化してから転送するようにした。このことにより、仮に、バスを第３者が観測し、保護されたデータを横取りしたとしても、そのデータを解読し平文化することを困難にすることが可能となる。
【０１８４】
そして、データを暗号化する際、初期ベクトルＩＶを適用するようにした。またその初期ベクトルＩＶは、乱数を用いてランダムに変更されるようにした。このようにすることで、仮に、第３者が何らかの方法で、保護されたデータを横取りしたとしても、そのデータを解読し平文化することをより困難にすることが可能となる。
【０１８５】
また、初期ベクトルＩＶが変更されるようすることで、平文データが特別なデータであることを特定させることを困難にすることが可能となる。このことは、データのすり替えや、データの改竄など、不正な行為を防止できることを意味する。さらに、初期ベクトルＩＶを適宜更新させることで、大量のデータを単一の鍵で暗号化した場合に、暗号鍵（セッションキーKs）が予測されやすくなるといった問題を解決することが可能となる。
【０１８６】
また、上述したように、本実施の形態によれば、ホスト３０２側から適切に初期ベクトルＩＶの更新が指示されなければ、データの供給が停止されるため、ドライブ装置３０１とホスト３０２との間で一旦、相互認証が成功したら、ドライブ装置３０１は、相手（ホスト３０２において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題を解決することができる。
【０１８７】
すなわち、正当なドライブ装置３０１は、正当なホスト３０２にのみ、保護されたデータを転送するように制御することが可能となる。
【０１８８】
上述した実施の形態においては、初期ベクトルＩＶが更新されるとしたが、暗号化に用いられるセッションキーKs自体が更新されるようにしても良い。換言すれば、ホスト３０２からは、初期ベクトルＩＶの再発行の指示が出されるのではなく、セッションキーKsの再発行の処理が出されるようにしても良い。
【０１８９】
しかしながら、セッションキーKsは、相互認証が正常に終了されなければ生成されないため、セッションキーKsの更新に係る処理時間や処理能力を考慮すると、初期ベクトルＩＶの方を更新する方が好ましいと考えられる。
【０１９０】
上述した実施の形態においては、ディスク３０３からデータを読み出す（再生）の場合を例に挙げて説明したが、本発明はデータの再生にのみ適用範囲が限定されるわけではない。すなわち、本発明を、ディスク３０３へのデータの書き込み（記録）に適用することも可能である。
【０１９１】
図１９は、本発明を記録装置に適用した場合のシステム構成例を示す図である。
【０１９２】
図１９に示し記録装置のドライブ装置４０１は、ホスト４０２から供給されるデータを、セットされているディスク３０３に記録する。ドライブ装置４０１は、認証処理部４１１、復号部４１２、セクタ転送制御部４１３、セクタ転送カウンタ４１４、乱数発生部４１５、メッセージ伝達部４１６、コマンド処理部４１７、および、アクセス処理部４１８を含む構成とされている。
【０１９３】

ホスト４０２は、認証処理部４２１、暗号化部４２２を含む構成とされている。

【０１９４】

図１９に示した記録装置の構成は、図１０に示した再生装置の構成と同様な部分が多いので、その詳細な説明は省略し、異なる部分についてのみ説明を加える。

【０１９５】

図１９に示した記録装置は、ディスク４０３にセクタデータを４５１を記録する。この記録されるセクタデータ４５１は、ホスト４０２側から供給されるセクタデータ４６１である。ホスト４０２の暗号化部４２２は、図示されていない記録媒体またはハードディスクドライブなどから読み出されたセクタデータ４６１を、認証処理部４２１から供給されるセッションキーKsを用いて暗号化する。

【０１９６】

暗号化部４２２により暗号化されたセクタデータ４６１は、ドライブ装置４０１のセクタ転送制御部４１３に供給される。セクタ転送制御部４１３は、供給されたセクタデータ４６１を、復号部４１２に供給する。復号部４１２は、供給されたセクタデータ４６１を、認証処理部４１１から供給されるセッションキーKsを用いて復号する。復号されたセクタデータ４６１は、セクタデータ４５１として、アクセス処理部４１８の制御のもと、ディスク４０３に記録される。

【０１９７】

セクタ転送カウンタ４１４は、セクタ転送制御部４１３から出力され、復号部４１２に供給されたセクタ数をカウントする。その他の部分に関しては、図１０に示した再生装置の対応する部分と、基本的に同様な構成であり、その動作も同様である。

【０１９８】

図１９に示した記録装置のドライブ装置４０１は、既に図１２、図１３のフローチャートを参照して説明した処理と、基本的に同様な処理を実行するため、詳細な説明は省略する。ここでは、再度、図１２、図１３のフローチャートを参照し、異なる処理のみに説明を加える。

【０１９９】

ドライブ装置４０１は、ステップＳ４４において、セクタデータの記録の要求があったか否かを判断する。この判断は、コマンド処理部４１７が、ホスト４０２側から、コマンドパケット４６３を受信したか否かを判断し、かつ、受信したコマンドパケット４６３が、セクタデータ４６１の書き込みを要求するもの（すなわち、ライトコマンド）であるか否かを判断することにより行われる。

【０２００】

また、ステップＳ４６においては、暗号化されたセクタデータ４６１が供給されるため、復号部４１２における復号処理が行われ、その復号されたセクタデータ４６１（４５１）がディスク４０３に書き込まれる処理が実行される。その他の処理については、基本的に同様であり、ホスト４０２から定期的に初期ベクトルＩＶの発行要求が出されなければ、ドライブ装置４０１側における書き込みの処理が停止される（ホスト４０３からのデータの出力が停止される）ように制御される。

【０２０１】

よって、ホスト４０２側で管理している保護されたデータが、不正に出力されること、そして、ディスク４０３に書き込まれてしまとことを防ぐことが可能となる。

【０２０２】

図２０のタイミングチャートを参照して、図１９に示した記録装置における、データの記録に関わる処理について説明を加えるが、基本的な処理は、図１７に示したタイミングチャートと同様であるので、その詳細な説明は省略する。異なる処理としては、ステップＳ３０１において、ホスト４０２から、データの書き込みを指示するライトコマンド（WRITE command）が送信される。

【０２０３】

また、ステップＳ３０２において、ホスト４０２の暗号化部４２２は、セクタデータ４

６１をセッションキーKsを用いて暗号化し、その暗号化したデータ（Encrypted Sector Data#１）を、ドライブ装置４０１に対して送信する。ドライブ装置４０１のセクタ転送制御部４２３は、供給されたEncrypted Sector Data ＃１を、復号部４１２に供給する。

【０２０４】

復号部４１２は、認証処理部４１１から供給されるセッションキーKsと、乱数発生部４１５から供給された初期ベクトルＩＶを用いて復号し、セクタデータ４５１を生成する。このようにして生成されたセクタデータ４５１は、アクセス処理部４１８の制御に基づき、ディスク４０３に書き込まれる。

【０２０５】

このような処理が行われると共に、セクタ転送カウンタ４１４は、セクタ転送制御部４１３から出力されたセクタ数をカウントする。そして、そのカウントされているカウンタ値Ｎが、Ｎmax以上になったか否かの判断を行う。カウンタ値Ｎが大きくなると、すなわち、セクタデータが、順次、セクタ転送制御部４１３から出力されると、カウンタ値Ｎの値が、閾値Ｎmaxよりも大きくなる（Ｎ＞Ｎmaxを満たす）ときがある。

【０２０６】

図２０を参照するに、（Ｎ１＋Ｎ２）＜Ｎmax＜（Ｎ１＋Ｎ２＋Ｎ３）と設定されていたとする。このような場合、ステップＳ３４０において、（Ｎ１＋Ｎ２＋１）番目のセクタデータが受信された後の時点（セクタ転送カウンタ４１４が管理するカウンタ値Ｎが、（Ｎ１＋Ｎ２＋１）となった後の時点）で、継続的に、セクタデータがディスク４０３に書き込まれるという処理が繰り返されると、カウンタ値Ｎの値は、順次１つづ増加されるので、Ｎ＞Ｎmaxという条件を満たすようになる。

【０２０７】

Ｎ＞Ｎmaxという条件が満たされると、すなわち、ステップＳ４５（図１３）において、ＹＥＳと判断されると、ステップＳ４８（図２０においては、ステップＳ３４１）に処理が進められる。

【０２０８】

ステップ４８（ステップＳ３４１）において、エラーメッセージ（Error Message）がドライブ装置４０１からホスト４０２側に出力される。ドライブ装置４０１のセクタ転送カウンタ４１４は、自己がカウントしているカウンタ値Ｎが、閾値Ｎmaxよりも大きくなったと判断したとき、セクタ転送制御部４１３に対して、復号部４１２にデータを出力しないように指示を出す。

【０２０９】

セクタ転送制御部４１３は、セクタ転送カウンタ４１４から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部４１６に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部４１６は、セクタ転送制御部４１３から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト４０２に対して送信する。このエラーメッセージは、ホスト４０２に、指示されたデータの書き込みはできないということを認識させるためのメッセージである。

【０２１０】

このようなメッセージが出力されると、ドライブ装置４０１側からはデータが入力されない状態とされる。また、エラーメッセージを受け取ったホスト４０２は、データを出力しない状態とされる。

【０２１１】

このように処理が行われることで、既に説明した再生装置の場合と同様の効果を望むことが可能である。

【０２１２】

このように、本発明を適用することにより、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。

【０２１３】

なお、上述した実施の形態においては、再生装置（図１０）と記録装置（図１９）をそ

れぞれ別な構成として図示および説明したが、再生装置と記録装置を同一の装置内に納めることも可能である。同一の装置内に納めるようにした場合、再生装置内と記録装置内において同一の処理を実行する、例えば、乱数発生部３１５（４１５）などは、再生装置と記録装置で共用される構成としても、もちろん良い。

【０２１４】

なお、上述した実施の形態においては、暗号化および復号の方式として、ＣＢＣ方式を例に挙げて説明したが、本発明は、ＣＢＣ方式にのみ適用できることを示すものではない。例えば、ＣＦＢ（Cipher Feed Back）方式、ＯＦＢ（Output Feed Block）方式などに対しても本発明を適用することはできる。

【０２１５】

上述した一連の処理は、それぞれの機能を有するハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【０２１６】

記録媒体は、その記録媒体を扱うパーソナルコンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM（Compact Disc-Read Only Memory），DVD（Digital Versatile Disc）を含む）、光磁気ディスク（MD（Mini-Disc）（登録商標）を含む）、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記憶されているＲＯＭやハードディスクなどで構成される。

【０２１７】

なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に従って、時系列的に行われる処理は勿論、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２１８】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

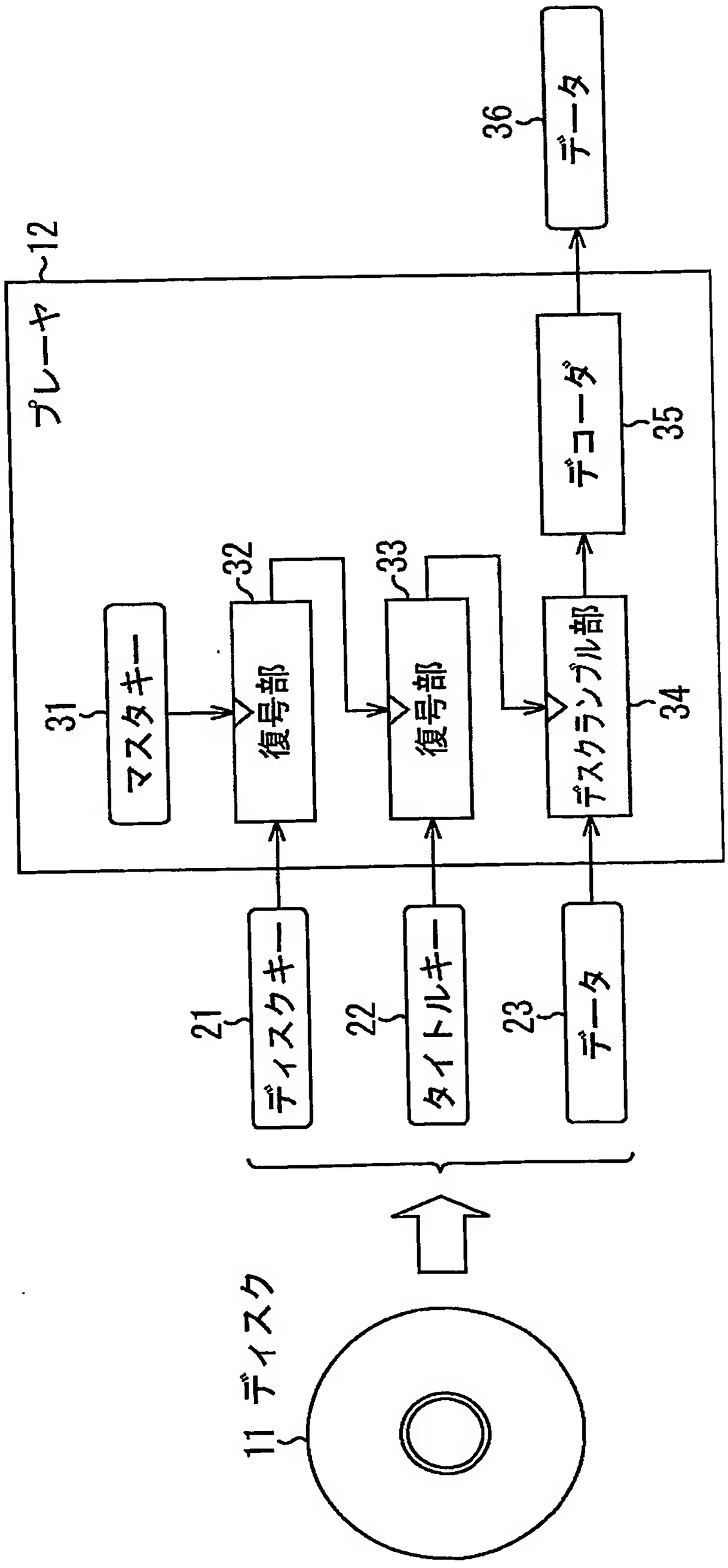
【図面の簡単な説明】

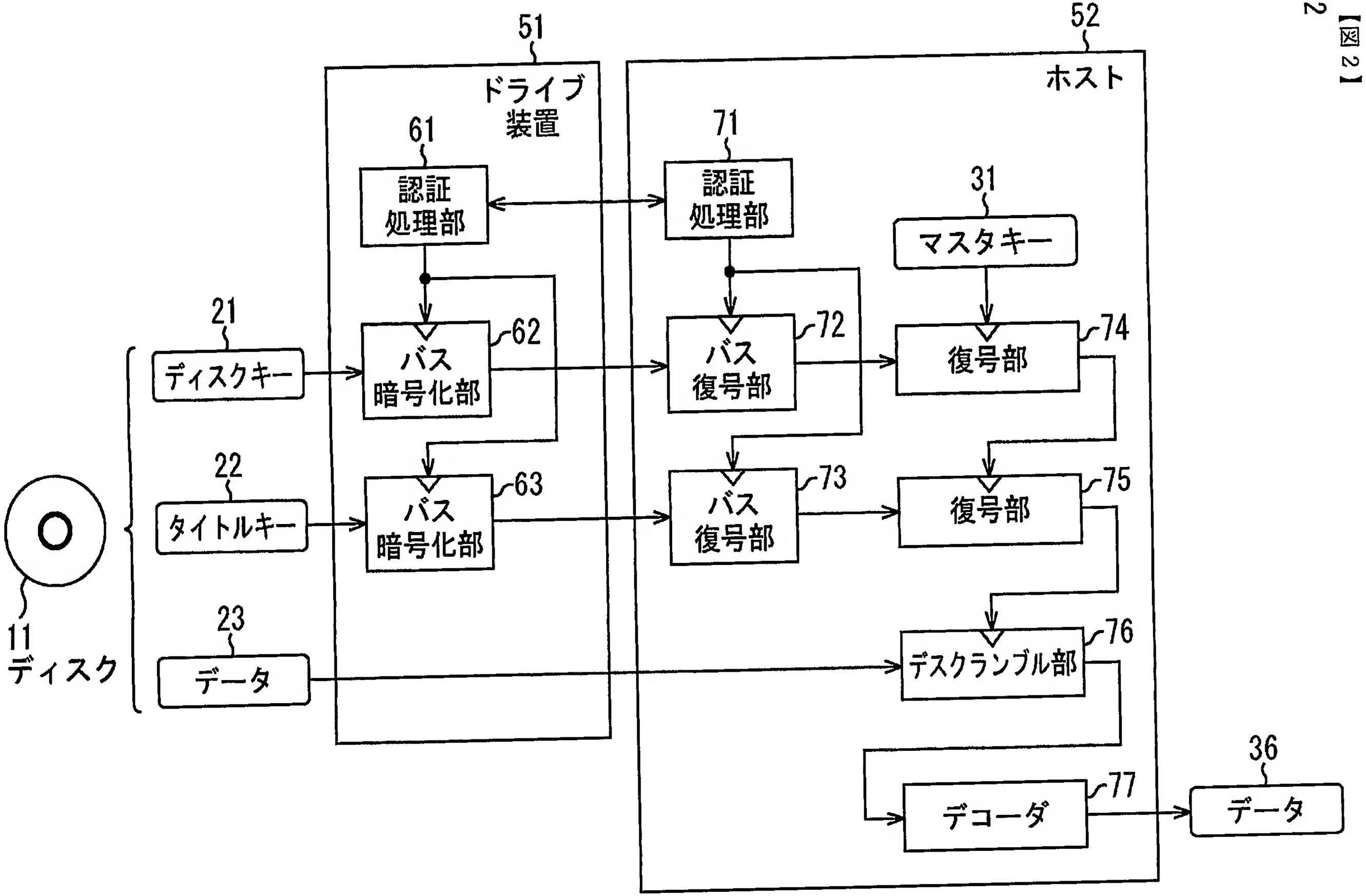
【０２１９】

【図１】従来の再生装置の一例の構成を示す図である。
【図２】従来の再生装置の他の構成例を示す図である。
【図３】認証処理について説明するためのフローチャートである。
【図４】暗号化を行う回路の構成例を示す図である。
【図５】復号を行う回路の構成例を示す図である。
【図６】従来の再生装置における問題点を説明するための図である。
【図７】従来の再生装置における問題点を説明するための図である。
【図８】初期ベクトルＩＶを授受する際の問題点を説明するための図である。
【図９】初期ベクトルＩＶを授受する際の問題点を説明するための図である。
【図１０】本発明を適用したシステムの一実施の形態の構成を示す図である。
【図１１】データの授受に係わるドライバーについて説明するための図である。
【図１２】ドライブ装置の動作について説明するためのフローチャートである。
【図１３】図１２のフローチャートに続くフローチャートである。
【図１４】初期ベクトルＩＶの授受に関するタイミングチャートである。
【図１５】初期ベクトルＩＶの授受に関するタイミングチャートである。
【図１６】初期ベクトルＩＶの授受に関するタイミングチャートである。
【図１７】データの授受に関するタイミングチャートである。

【図１８】コマンドパケットの構成を示す図である。
【図１９】本発明を適用したシステムの他の実施の形態の構成を示す図である。
【図２０】データの授受に関するタイミングチャートである。
【符号の説明】
【０２２０】
３０１　ドライブ装置，　３０２　ホスト，　３０３　ディスク，　３１１　認証処理部，　３１２　暗号化部，　３１３　セクタ転送制御部，　３１４　セクタ転送カウンタ部，　３１５　乱数発生部，　３１６　メッセージ伝達部，　３１７　コマンド処理部，　３１８　アクセス処理部，　３２１　認証処理部、　３２２　復号部，　４０１　ドライブ装置，　４０２　ホスト，　４０３　ディスク，　４１１　認証処理部，　４１２　復号部，　４１３　セクタ転送制御部，　４１４　セクタ転送カウンタ，　４１５　乱数発生部，　４１６　メッセージ伝達部，　４１７　コマンド処理部，　４１８　アクセス処理部，　４２１　認証処理部、　４２２　暗号化部

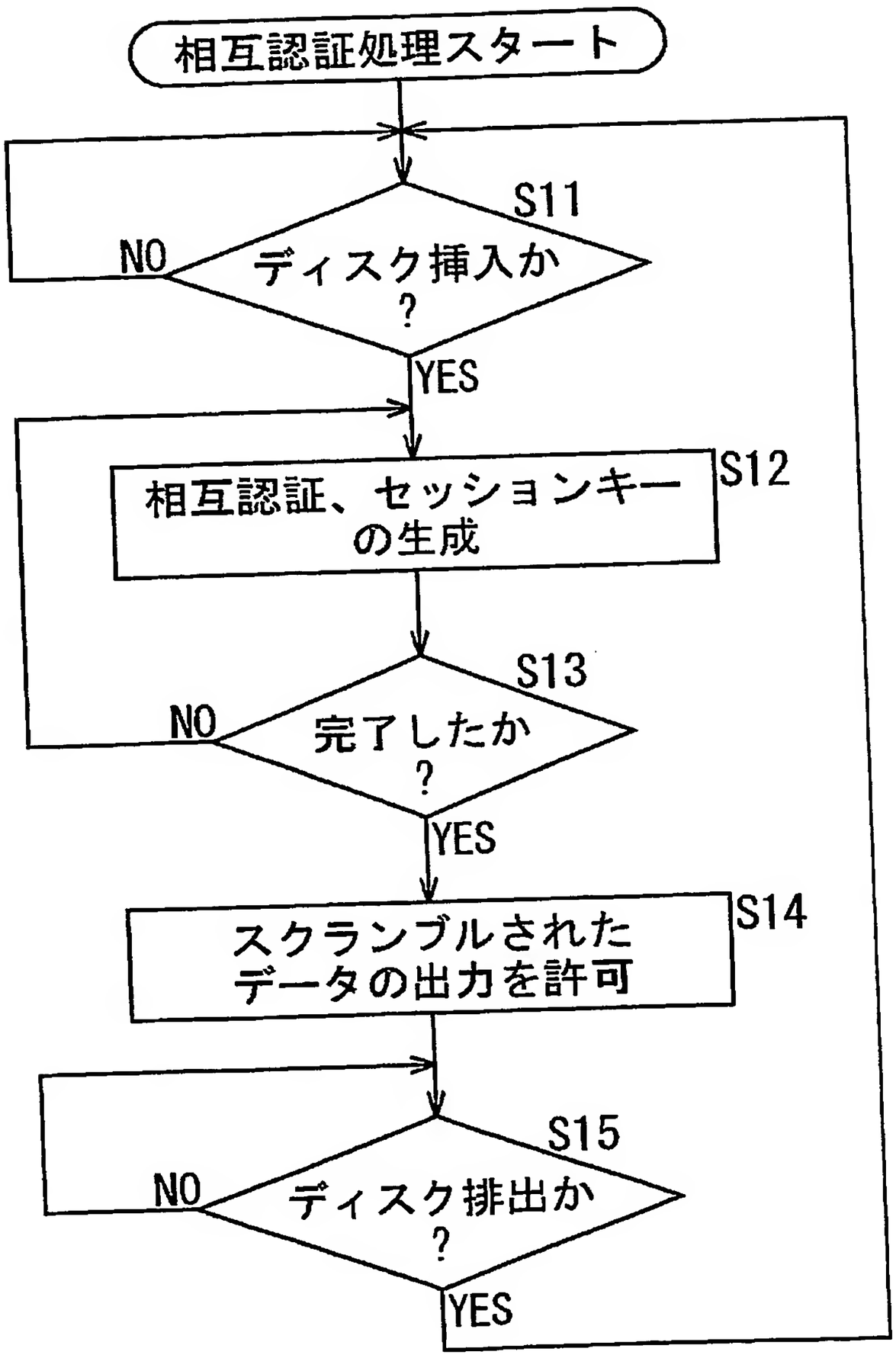
【書類名】図面
【図１】
図1


11 ディスク
プレーヤ
12
31 マスタキー
32 復号部
33 復号部
デスクランブル部
34
21 ディスクキー
22 タイトルキー
23 データ
35 デコーダ
36 データ


51
ドライブ装置
52
ホスト
61
認証処理部
71
認証処理部
31
マスタキー
21
ディスクキー
62
バス暗号化部
72
バス復号部
74
復号部
22
タイトルキー
63
バス暗号化部
73
バス復号部
75
復号部
11
ディスク
23
データ
76
デスクランブル部
77
デコーダ
36
データ

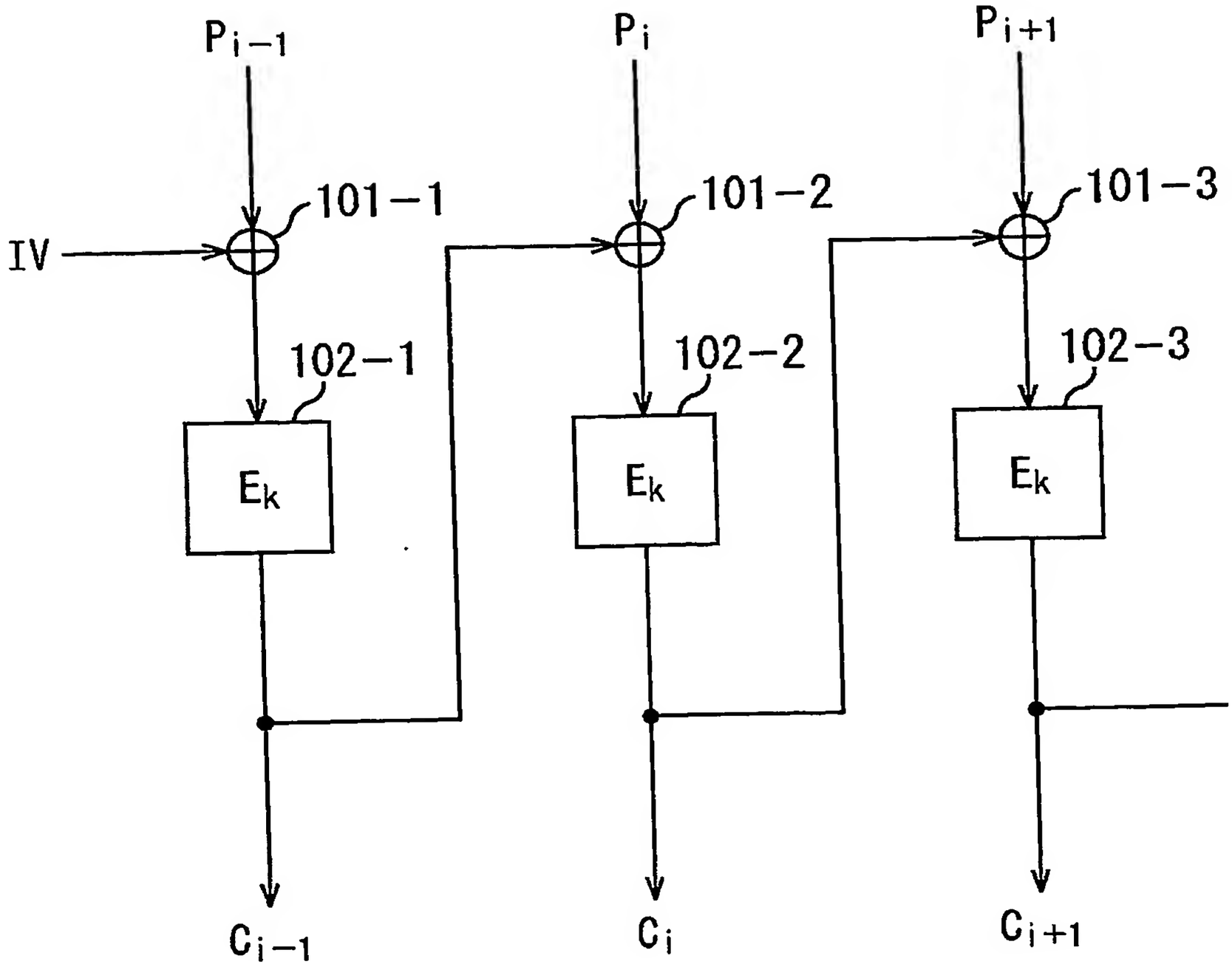
【図３】

図3

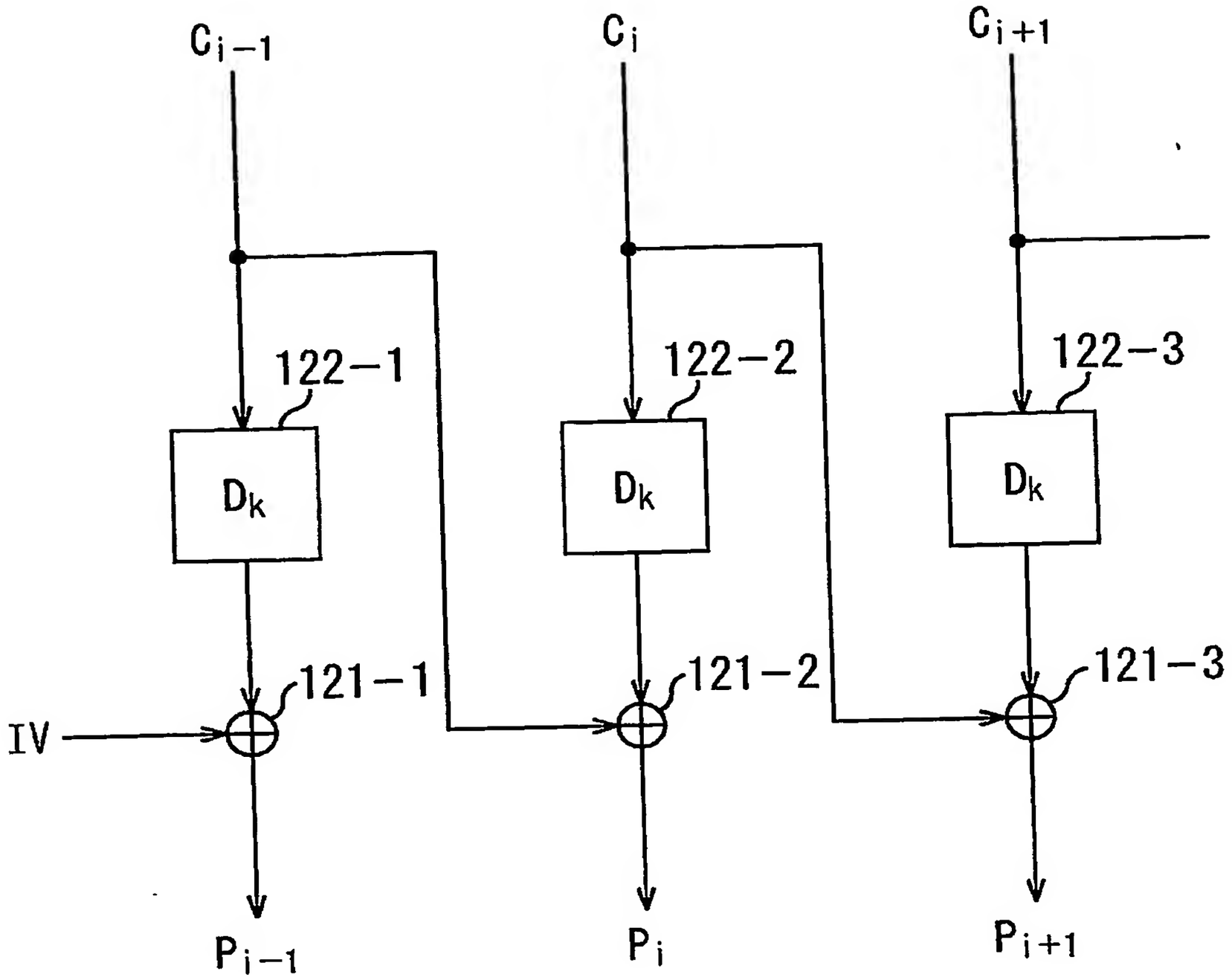

相互認証処理スタート
S11
NO
ディスク挿入か
?
YES
S12
相互認証、セッションキー
の生成
S13
NO
完了したか
?
YES
S14
スクランブルされた
データの出力を許可
S15
NO
ディスク排出か
?
YES

【図４】

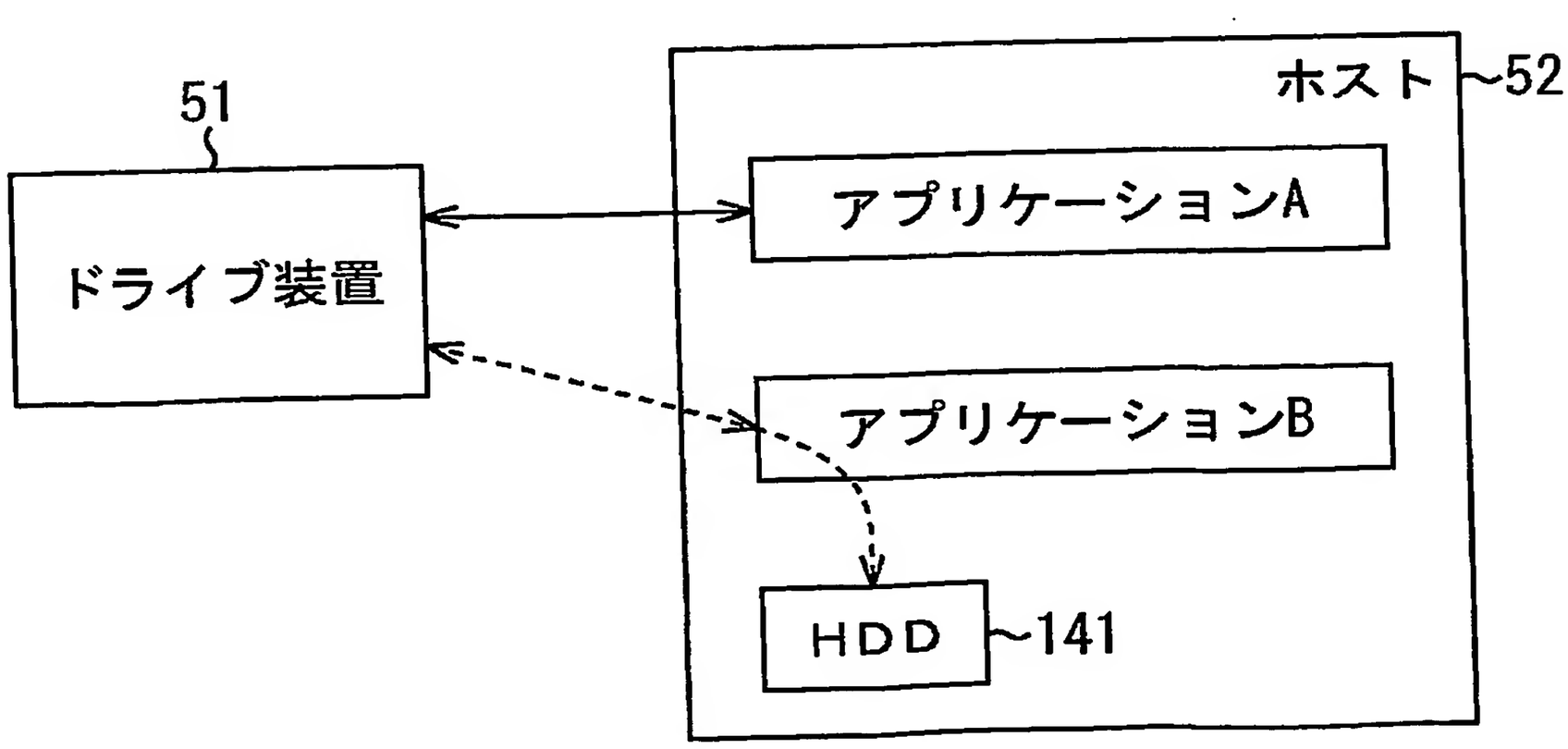
図4



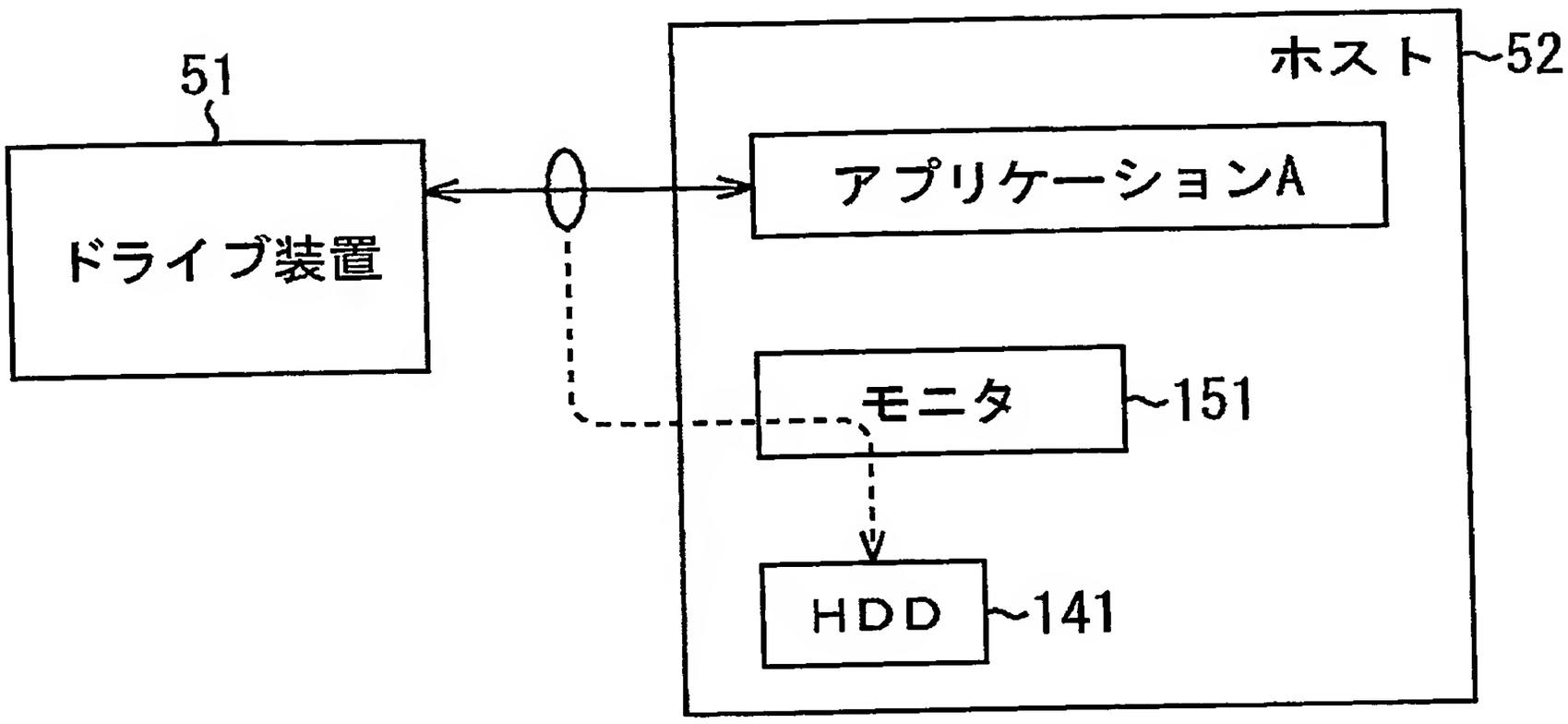
【図５】
図5


Ci−1
Ci
Ci+1
122−1
122−2
122−3
Dk
Dk
Dk
121−1
121−2
121−3
IV
Pi−1
Pi
Pi+1

【図６】
図6

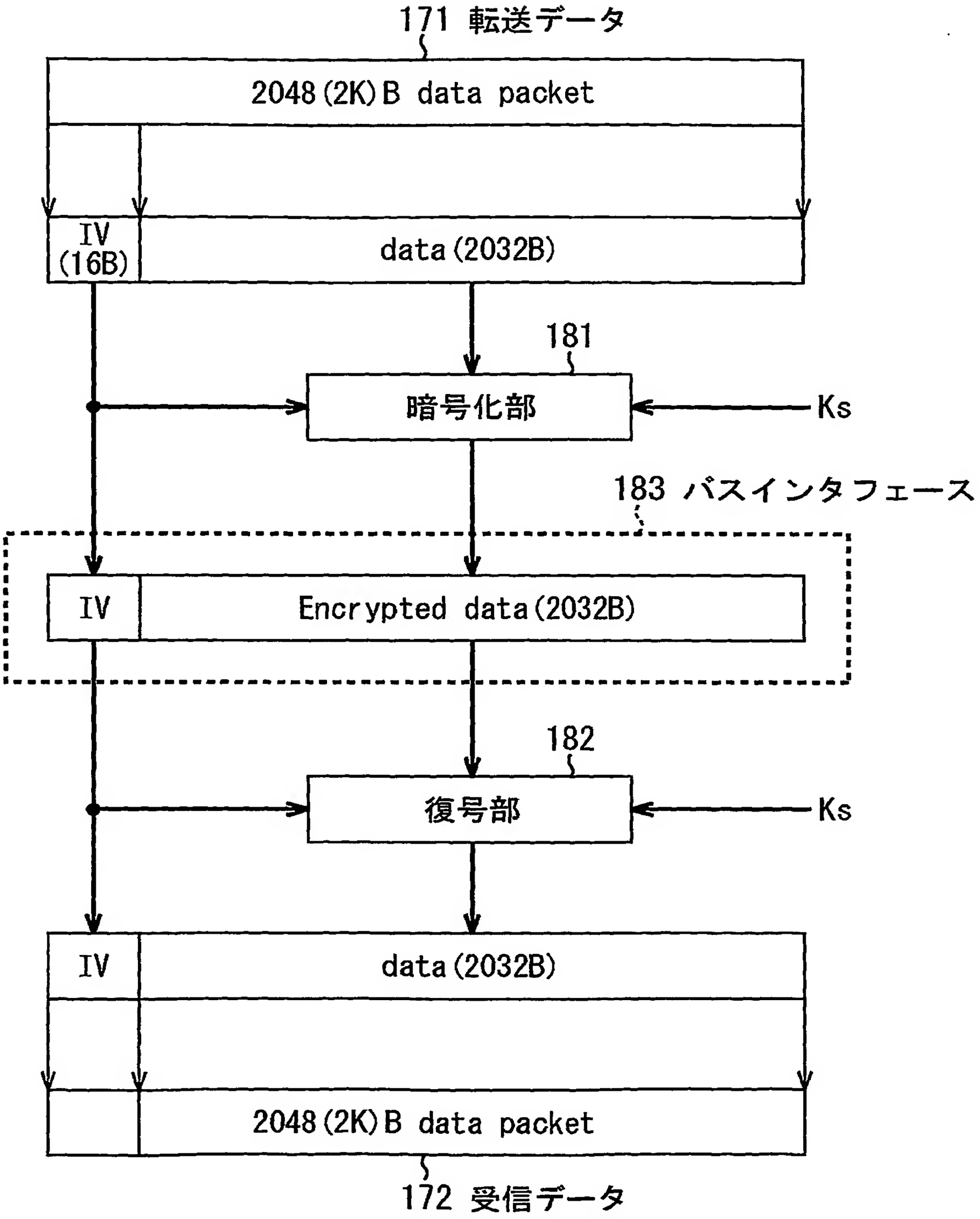

51
ドライブ装置
ホスト
52
アプリケーションA
アプリケーションB
HDD
141

【図７】
図7



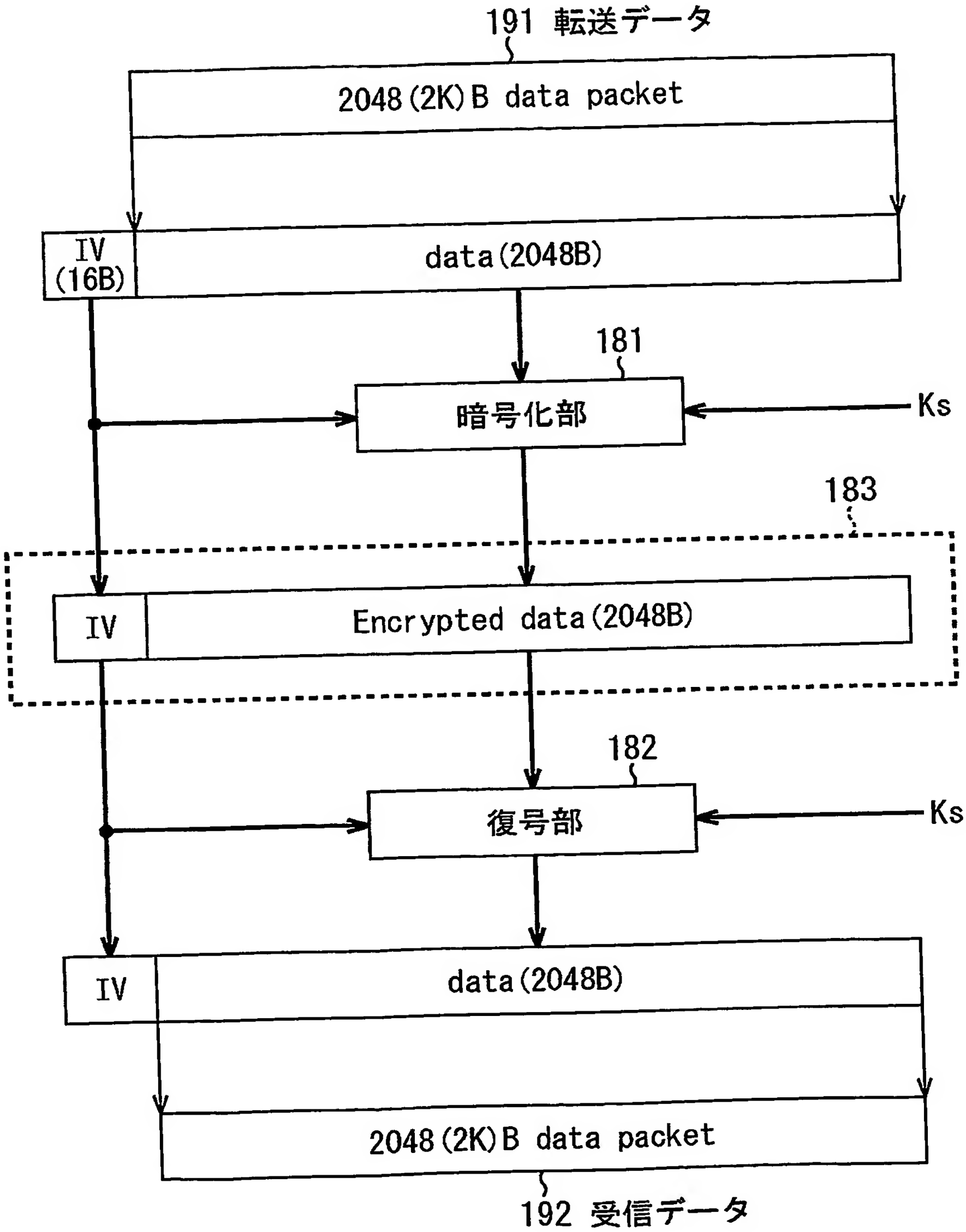
【図８】

図8


171 転送データ
2048(2K)B data packet
IV
(16B)
data(2032B)
181
暗号化部
Ks
183 パスインタフェース
IV
Encrypted data(2032B)
182
復号部
Ks
IV
data(2032B)
2048(2K)B data packet
172 受信データ

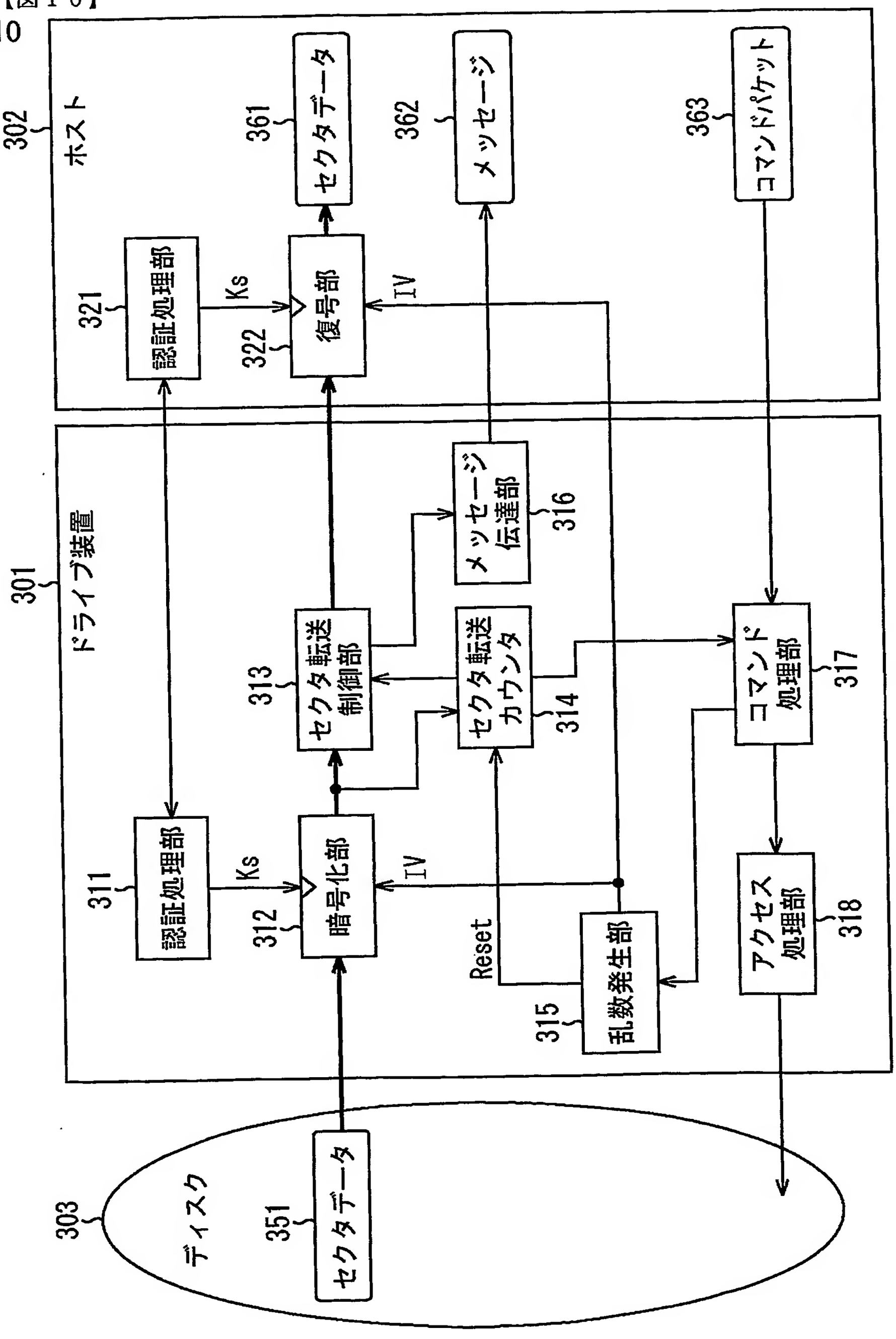
【図９】

図9


191 転送データ
2048(2K)B data packet
IV (16B)
data(2048B)
181
暗号化部
Ks
183
IV
Encrypted data(2048B)
182
復号部
Ks
IV
data(2048B)
2048(2K)B data packet
192 受信データ

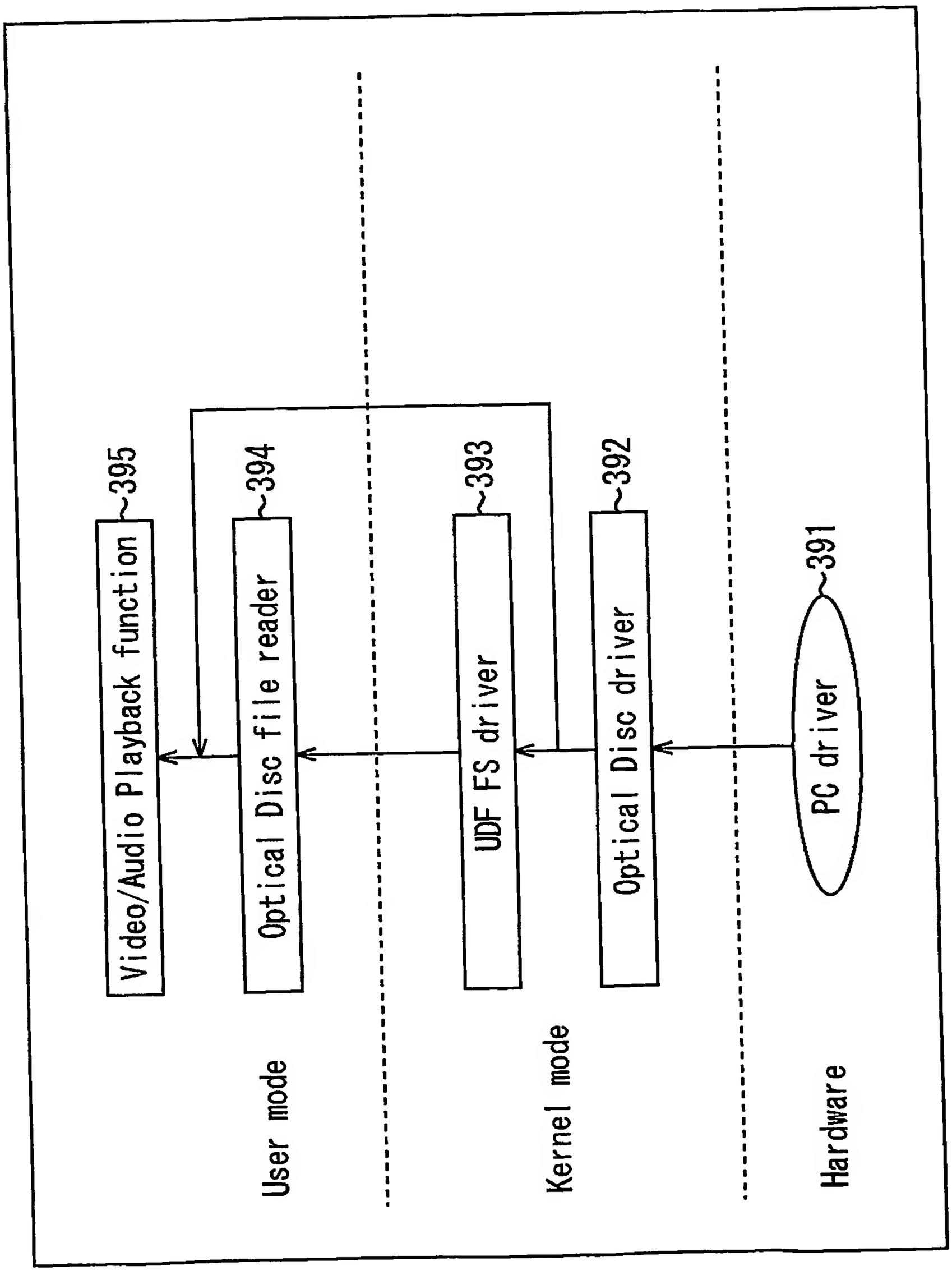
【図１０】

図10


302
ホスト
361
セクタデータ
362
メッセージ
363
コマンドパケット
321
認証処理部
Ks
322
復号部
IV
301
ドライブ装置
メッセージ伝達部
316
313
セクタ転送制御部
セクタ転送カウンタ
314
コマンド処理部
317
311
認証処理部
Ks
312
暗号化部
IV
Reset
315
乱数発生部
アクセス処理部
318
303
ディスク
351
セクタデータ

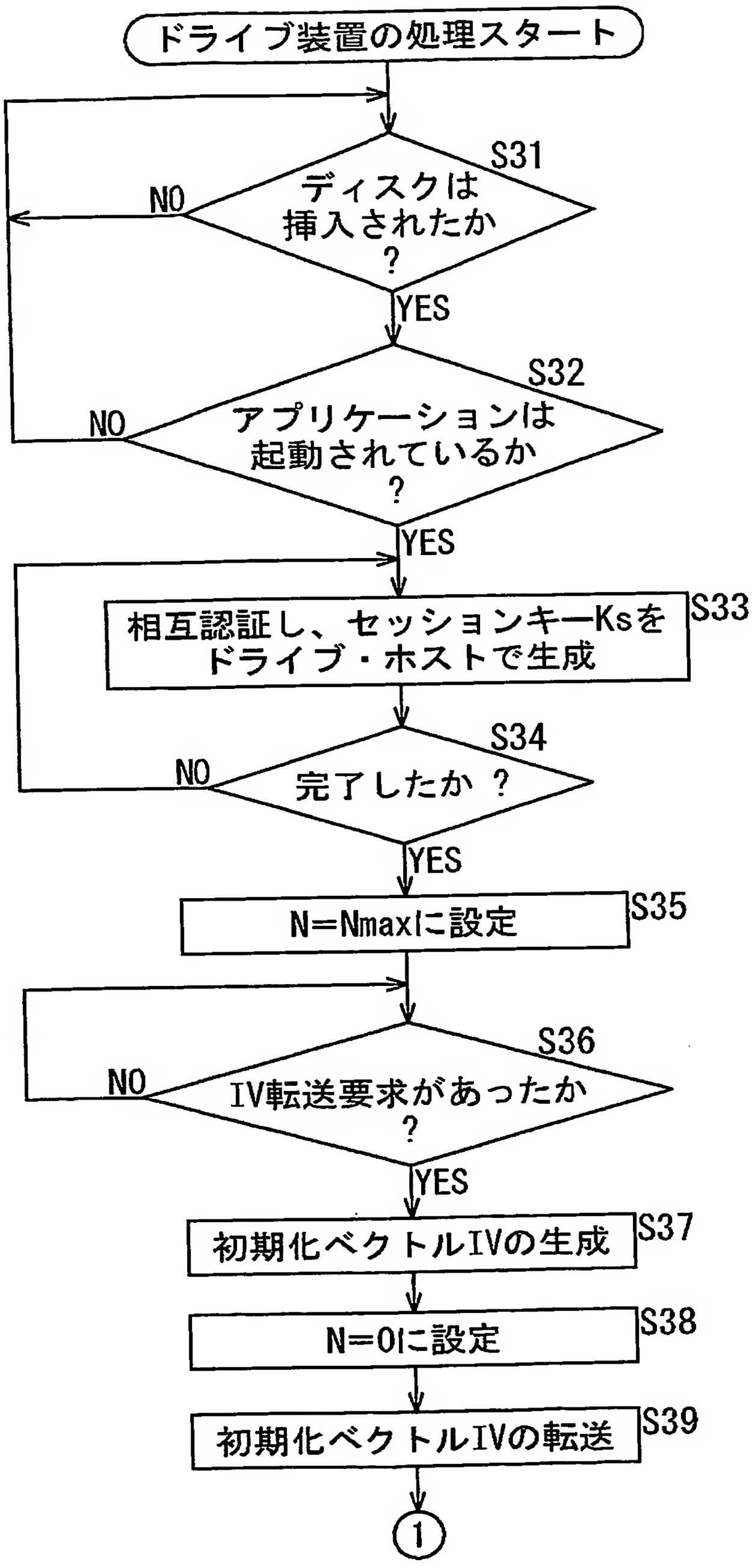
【図１１】

図11


Video/Audio Playback function
395
Optical Disc file reader
394
UDF FS driver
393
Optical Disc driver
392
PC driver
391
User mode
Kernel mode
Hardware

【図１２】

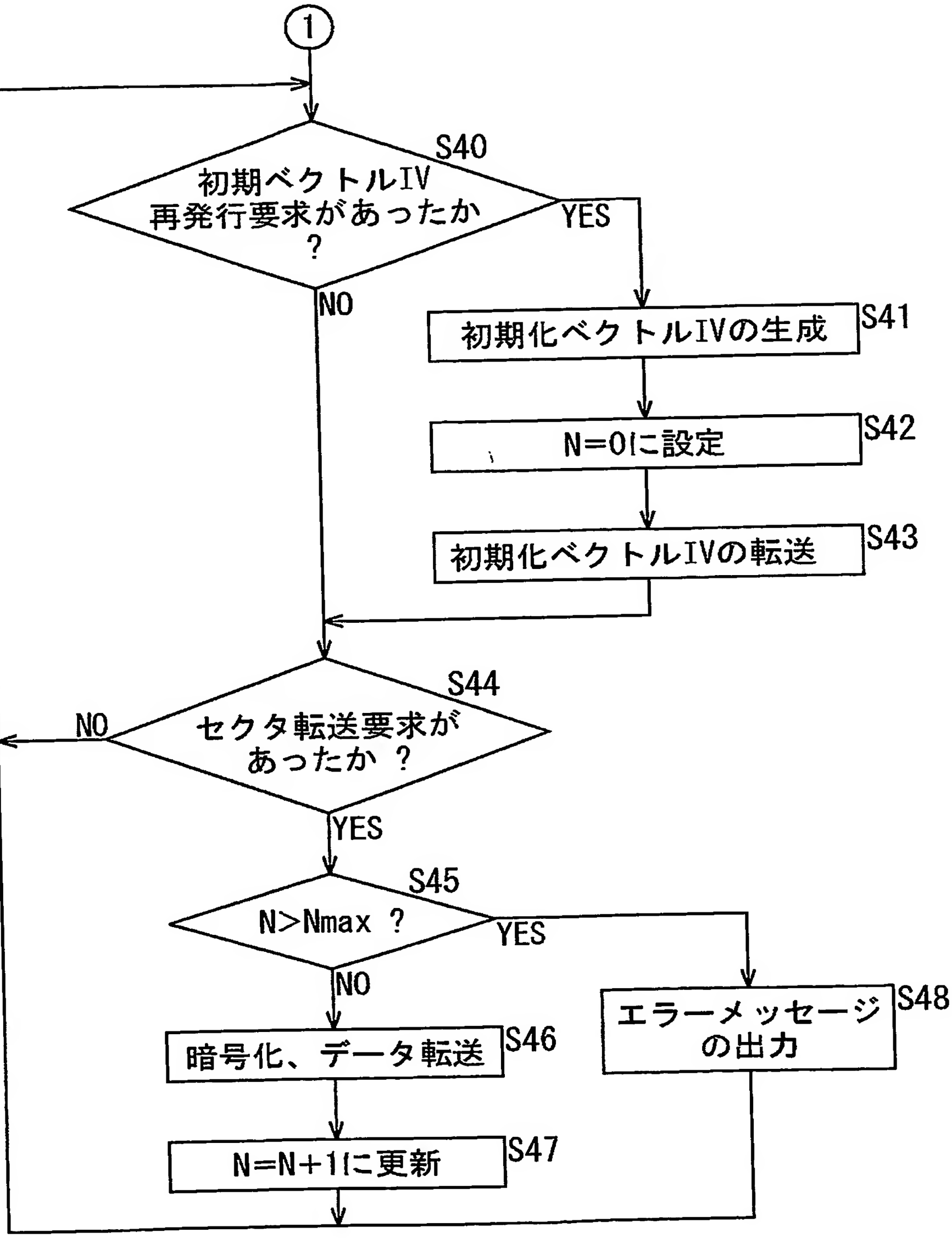
図12
(12−1)


ドライブ装置の処理スタート
S31
ディスクは挿入されたか？
NO
YES
S32
アプリケーションは起動されているか？
NO
YES
S33
相互認証し、セッションキーKsをドライブ・ホストで生成
S34
完了したか？
NO
YES
S35
N=Nmaxに設定
S36
IV転送要求があったか？
NO
YES
S37
初期化ベクトルIVの生成
S38
N=0に設定
S39
初期化ベクトルIVの転送
①

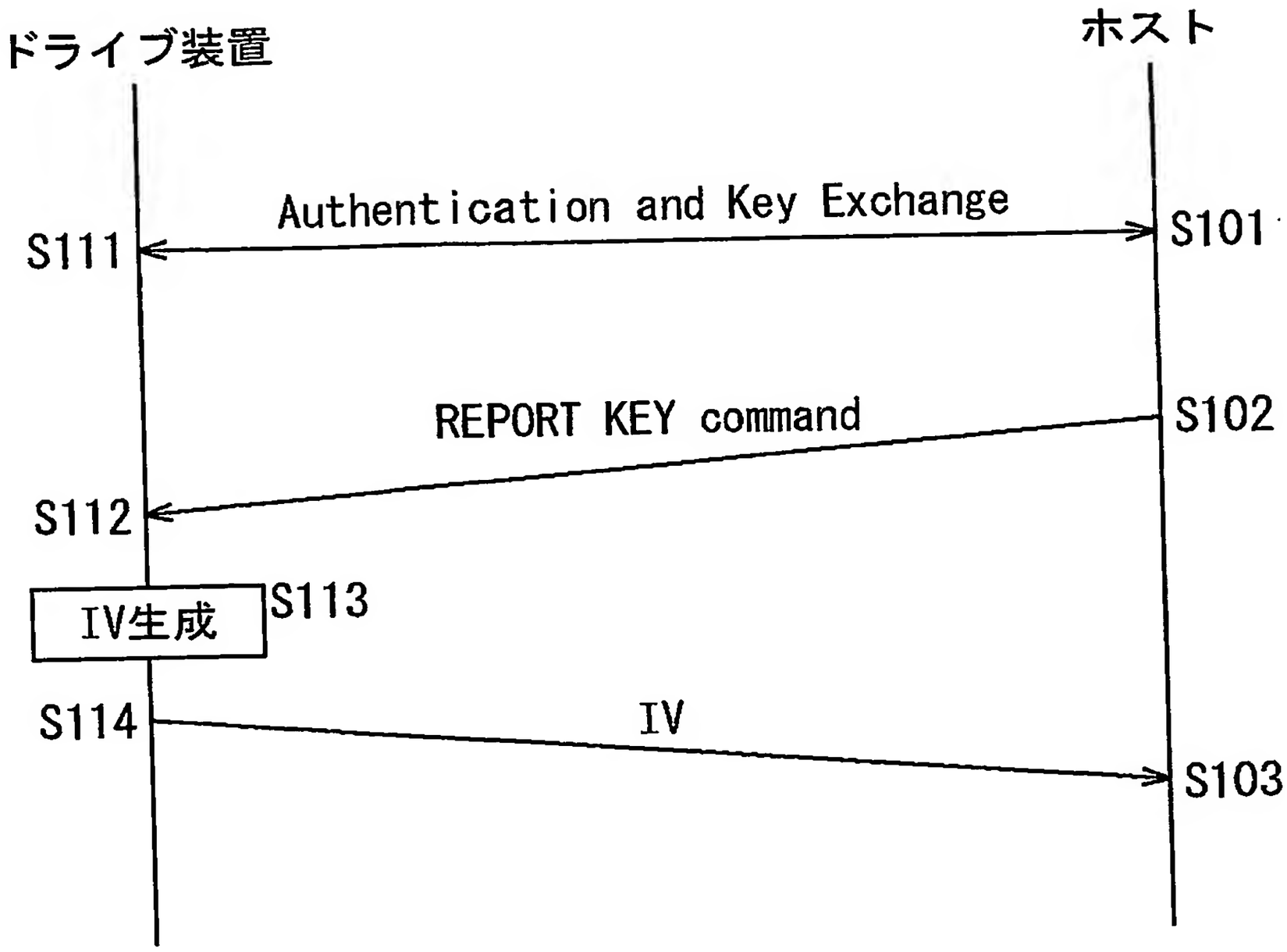
【図１３】

図13

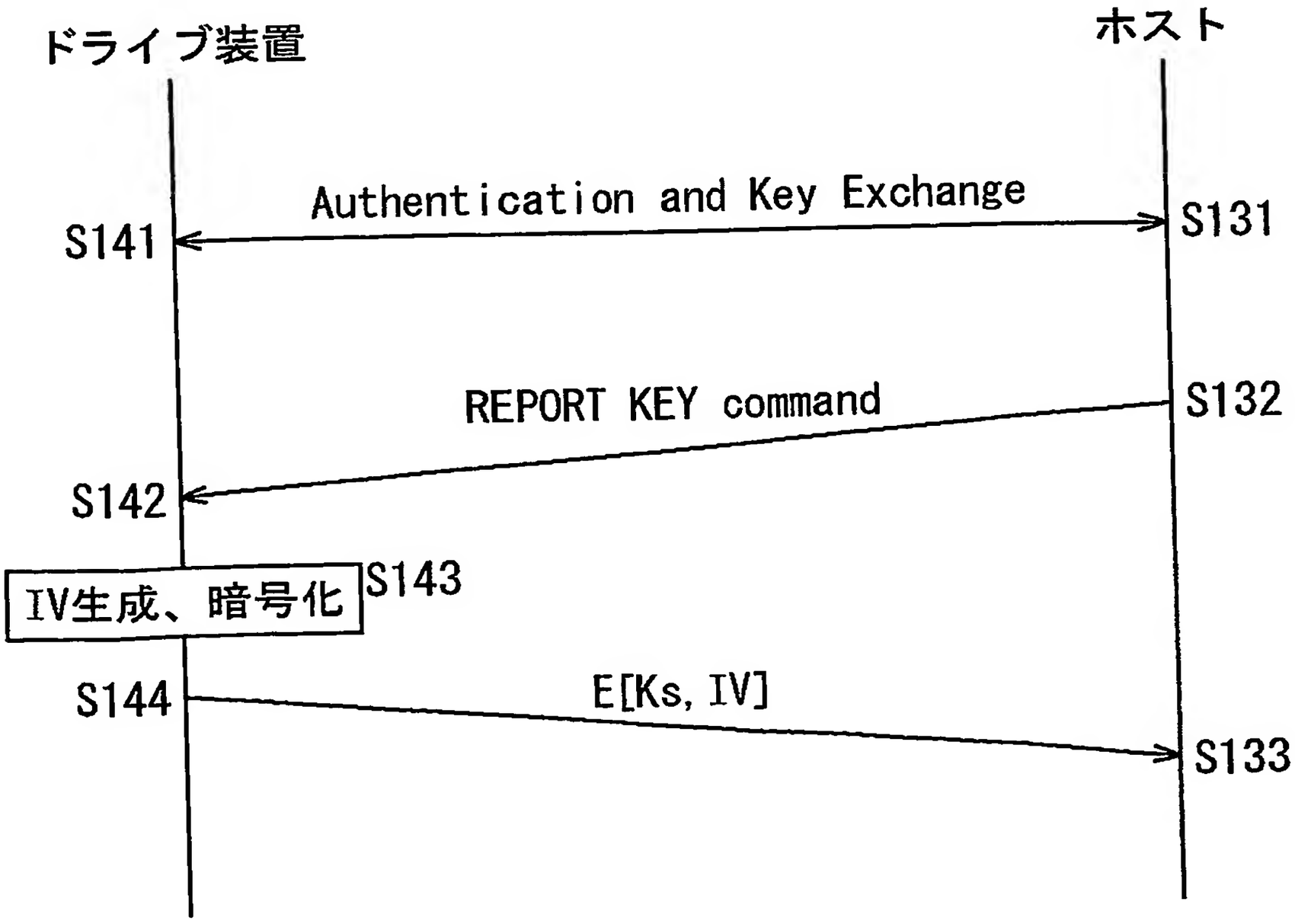
(12−2)


1
S40
初期ベクトルIV
再発行要求があったか
？
YES
NO
S41
初期化ベクトルIVの生成
S42
N=0に設定
S43
初期化ベクトルIVの転送
S44
NO
セクタ転送要求が
あったか ？
YES
S45
N>Nmax ？
YES
NO
S46
暗号化、データ転送
S47
N=N+1に更新
S48
エラーメッセージ
の出力

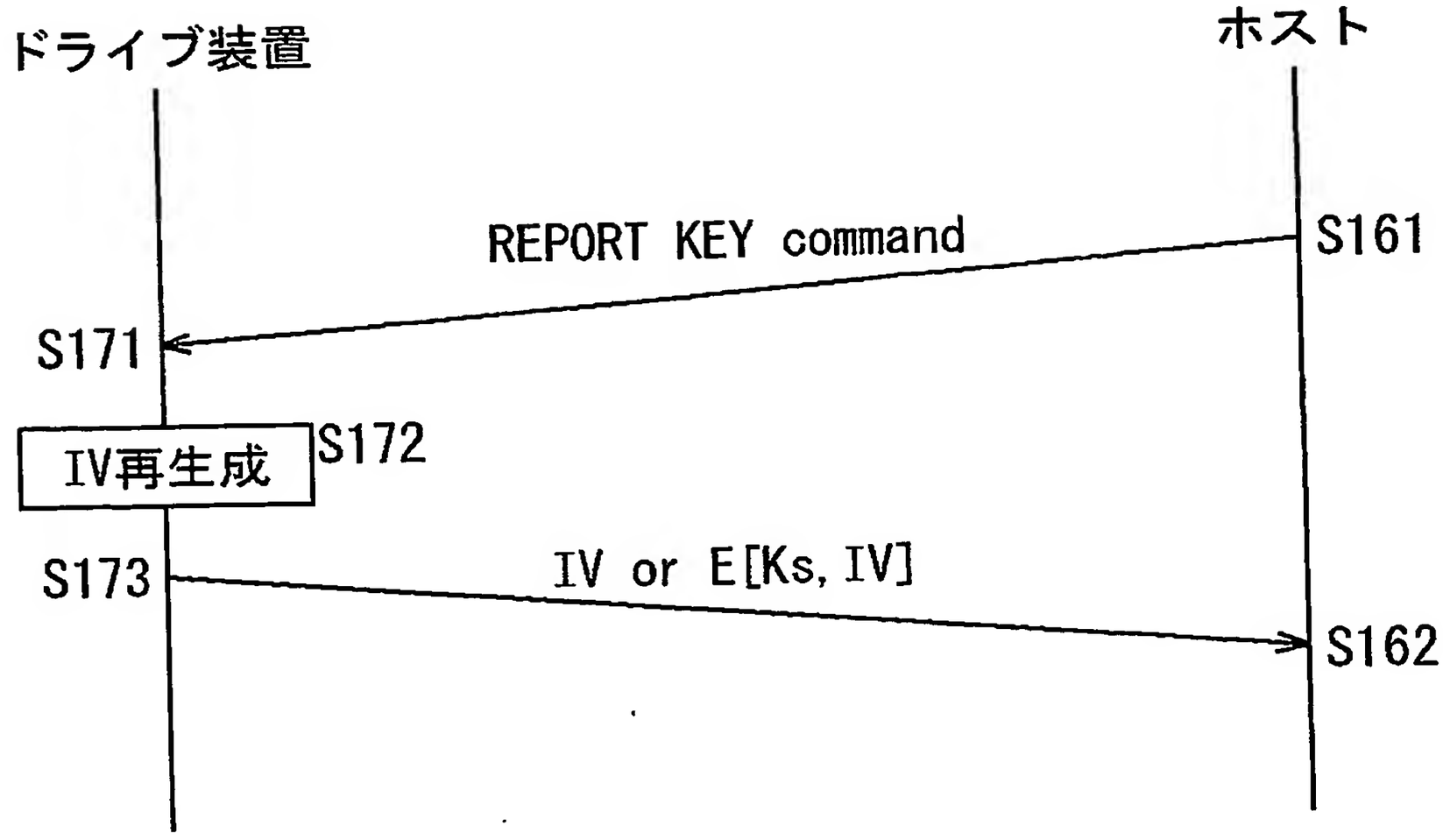
【図１４】
図14



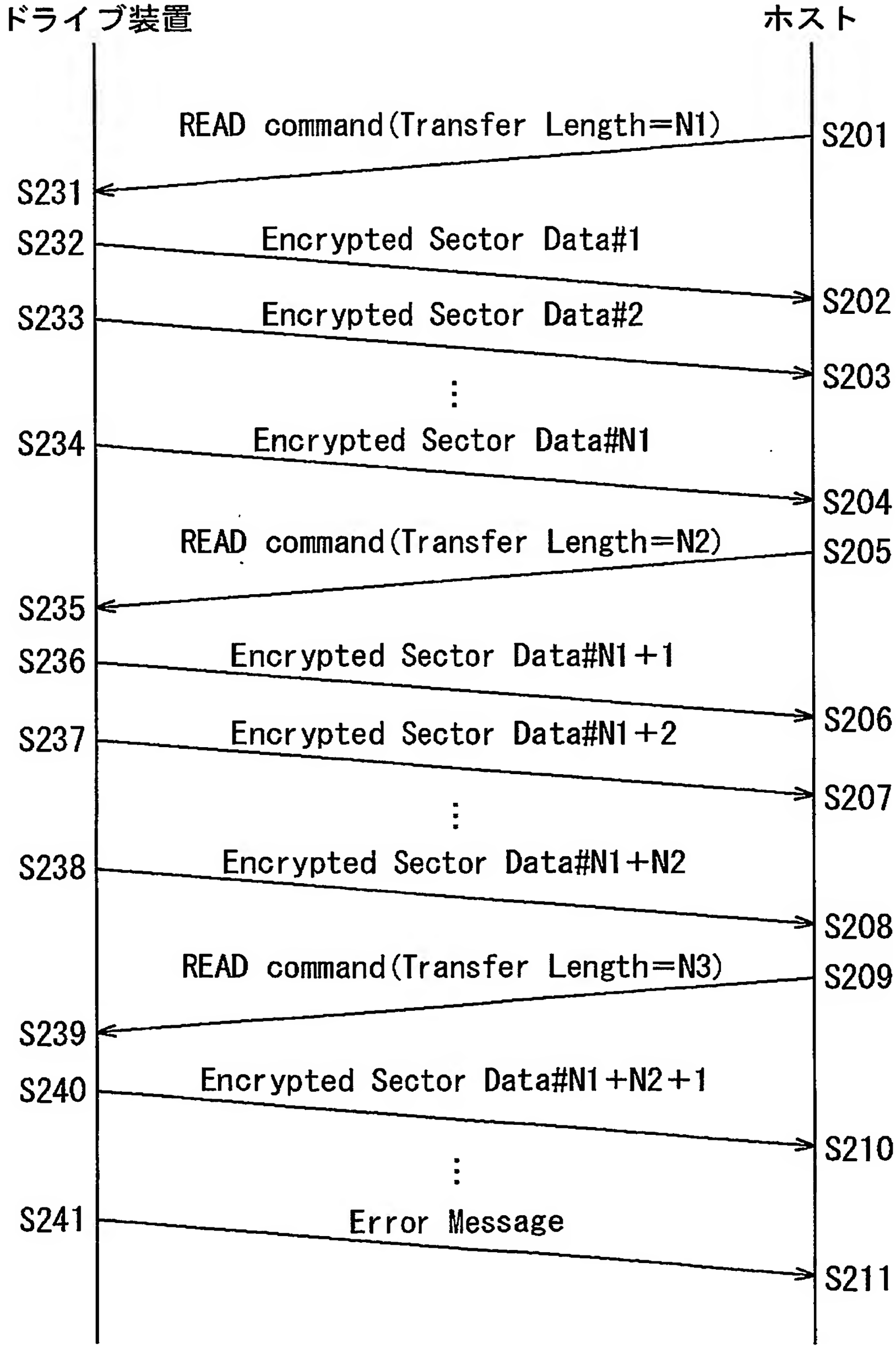
【図１５】
図15



【図１６】
図16


ドライブ装置
ホスト
REPORT KEY command
S161
S171
IV再生成
S172
S173
IV or E[Ks, IV]
S162

【図１７】
図17


ドライブ装置
ホスト
READ command(Transfer Length=N1)
S201
S231
S232
Encrypted Sector Data#1
S202
S233
Encrypted Sector Data#2
S203
S234
Encrypted Sector Data#N1
S204
READ command(Transfer Length=N2)
S205
S235
S236
Encrypted Sector Data#N1+1
S206
S237
Encrypted Sector Data#N1+2
S207
S238
Encrypted Sector Data#N1+N2
S208
READ command(Transfer Length=N3)
S209
S239
S240
Encrypted Sector Data#N1+N2+1
S210
S241
Error Message
S211

【図１８】

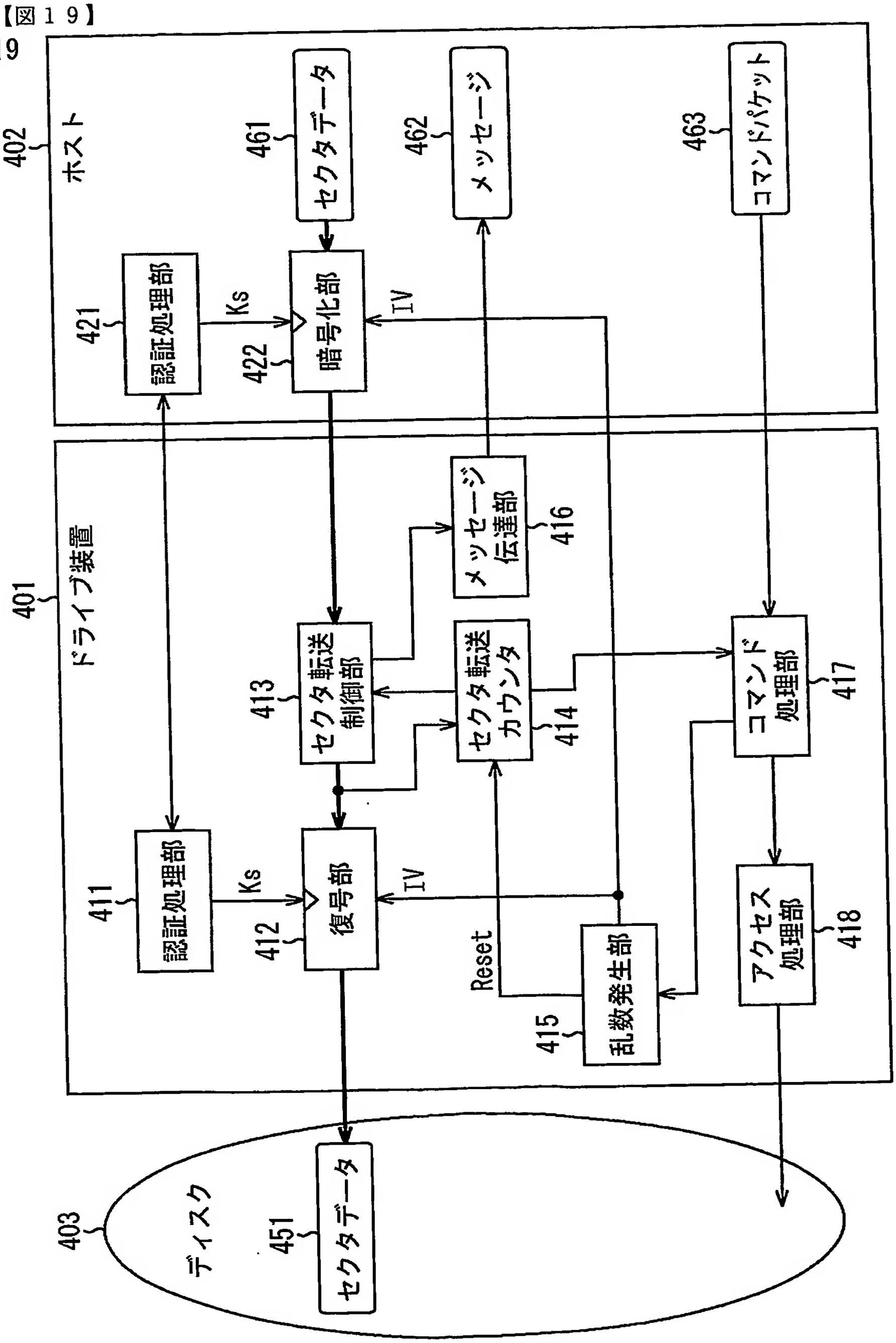
図18

363

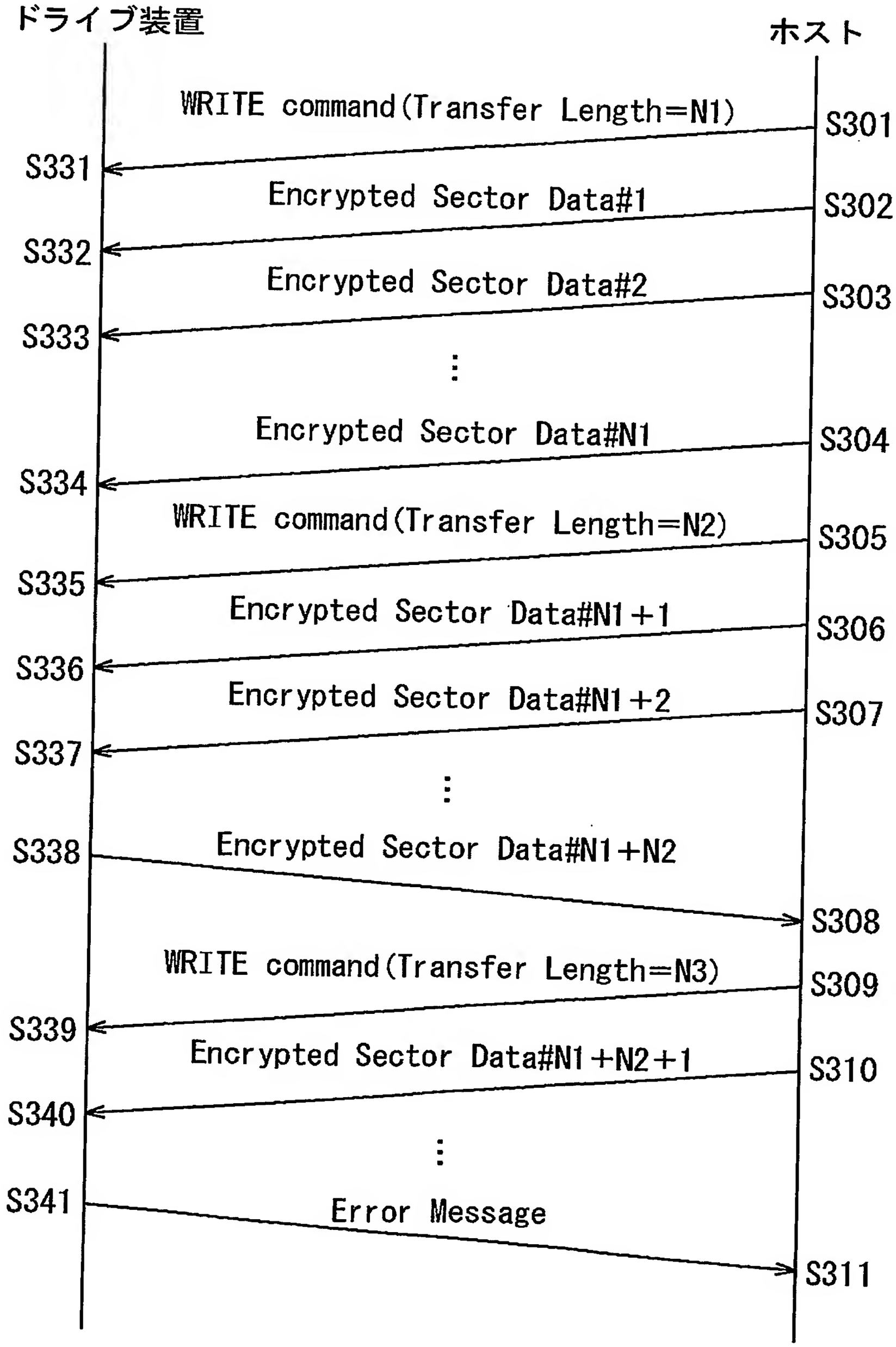
Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code							
1	LUN (Obsolete)			DPO(0)	FUA	Reserved		RelAdr
2	(MSB) Logical Block Address							
3								
4								
5								(LSB)
6	(MSB) Transfer Length							
7								
8								(LSB)
9	Control							
10	Streaming		Reserved					
11	Vendor－Spacific			Reserved			Flag	Link

【図１９】

図19


402
ホスト
461
セクタデータ
462
メッセージ
463
コマンドパケット
421
認証処理部
Ks
422
暗号化部
IV
401
ドライブ装置
メッセージ伝達部
416
413
セクタ転送制御部
セクタ転送カウンタ
414
コマンド処理部
417
411
認証処理部
Ks
412
復号部
IV
Reset
415
乱数発生部
アクセス処理部
418
403
ディスク
451
セクタデータ

【図２０】
図20


ドライブ装置
ホスト
WRITE command(Transfer Length=N1)
S301
S331
Encrypted Sector Data#1
S302
S332
Encrypted Sector Data#2
S303
S333
Encrypted Sector Data#N1
S304
S334
WRITE command(Transfer Length=N2)
S305
S335
Encrypted Sector Data#N1+1
S306
S336
Encrypted Sector Data#N1+2
S307
S337
Encrypted Sector Data#N1+N2
S338
S308
WRITE command(Transfer Length=N3)
S309
S339
Encrypted Sector Data#N1+N2+1
S310
S340
Error Message
S341
S311

【書類名】要約書
【要約】
【課題】　データの授受をセキュリティを高めた状態で行えるようにする。
【解決手段】　ホストとドライブ装置は、所定のバスで接続されており、そのバスを介してデータの授受を行う。ホストは、ドライブ装置に対して、バス上を介して授受されるデータを暗号化および復号の際に用いられる初期ベクトルＩＶの発行の要求を定期的に行う。ドライブ装置は、要求があったとき、初期ベクトルＩＶを生成しホストに供給する。このような処理が定期的に行われなければ、ドライブ装置は、ホストに対するデータの出力を停止する。本発明は、記録媒体に記録されているデータを再生するドライブ装置を有するパーソナルコンピュータに適用することが可能である。
【選択図】図１６

特願２００４－００４７９８

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000061

International filing date: 06 January 2005 (06.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-004798
Filing date: 09 January 2004 (09.01.2004)

Date of receipt at the International Bureau: 04 February 2005 (04.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse